Number Theory Notes

St. Joseph's University

Asher Roberts

Contents

Chapter 1

Preliminaries

1.1 Mathematical Induction

Well-Ordering Principle. Every nonempty set S of nonnegative integers contains a least element; that is, there is some integer a in S such that $a \leq b$ for all b's belonging to S.

Theorem 1.1.1 (Archimedean property)**.** *If a and b are any positive integers, then there exists a positive integer n such that $na \geq b$.*

Proof. Assume that the statement of the theorem is not true, so that for some a and b, $na < b$ for every positive integer n. Then the set

$$S = \{b - na \mid n \text{ a positive integer}\}$$

consists entirely of positive integers. By the Well-Ordering Principle, S will possess a least element, say $b - ma$. Notice that $b - (m + 1)a$ also lies in S, because S contains all integers of this form. Furthermore, we have

$$b - (m + 1)a = (b - ma) - a < b - ma$$

contrary to the choice of $b - ma$ as the smallest integer in S. This contradiction arose out of our original assumption that the Archimedean property did not hold; hence, this property is proven true. □

Theorem 1.1.2 (First Principle of Finite Induction)**.** *Let S be a set of positive integers with the following properties:*

(a) The integer 1 *belongs to S.*

(b) Whenever the integer k is in S, the next integer $k+1$ must also be in S.

Then S is the set of all positive integers.

Proof. Let T be the set of all positive integers not in S, and assume that T is nonempty. The Well-Ordering Principle tells us that T possesses a least element, which we denote by a. Because 1 is in S, certainly $a > 1$, and so $0 < a - 1 < a$. The choice of a as the smallest positive integer in T implies that $a - 1$ is not a member of T, or equivalently that $a - 1$ belongs to S. By hypothesis, S must also contain $(a - 1) + 1 = a$, which contradicts the fact that a lies in T. We conclude that the set T is empty and in consequence that S contains all the positive integers. □

Example 1. Prove that

$$1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(2n+1)(n+1)}{6}$$

for $n = 1, 2, 3, \ldots$.

Example 2. Find a formula for

$$1 + 2 + 2^2 + 2^3 + \cdots + 2^{n-1}$$

for every positive integer n.

Remark 1. As with the first version, the Second Principle of Finite Induction gives two conditions that guarantee a certain set of positive integers actually consists of all positive integers. We retain requirement (a), but (b) is replaced by
(b') If k is a positive integer such that $1, 2, \ldots, k$ belong to S, then $k+1$ must also be in S.

Example 3. Consider the so-called Lucas sequence:

$$1, 3, 4, 7, 11, 18, 29, 47, 76, \ldots.$$

Except for the first two terms, each term of this sequence is the sum of the preceding two, so that the sequence may be defined inductively by

$$\begin{aligned} a_1 &= 1 \\ a_2 &= 3 \\ a_n &= a_{n-1} + a_{n-2} \qquad \text{for all } n \geq 3. \end{aligned}$$

Show that the inequality

$$a_n < (7/4)^n$$

holds for every positive integer n.

1.2 The Binomial Theorem

Definition 1.2.1. For any positive integer n and any integer k satisfying $0 \leq k \leq n$, the binomial coefficients are defined by

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}.$$

Example 1. Prove Pascal's rule:

$$\binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k} \qquad 1 \leq k \leq n.$$

Theorem 1.2.1 (Binomial Theorem)**.** *The complete expansion of* $(a+b)^n$*,* $n \geq 1$*, is given by*

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k$$

Proof. Mathematical induction provides the best means for confirming this formula. When $n = 1$, the conjectured formula reduces to

$$(a+b)^1 = \sum_{k=0}^{1} \binom{1}{k} a^{1-k} b^k = \binom{1}{0} a^1 b^0 + \binom{1}{1} a^0 b^1 = a + b,$$

which is certainly correct. Assuming that the formula holds for some fixed integer m, we go on to show that it also must hold for $m+1$. The starting point is to notice that

$$(a+b)^{m+1} = a(a+b)^m + b(a+b)^m.$$

Under the induction hypothesis,

$$\begin{aligned} a(a+b)^m &= \sum_{k=0}^{m} \binom{m}{k} a^{m-k+1} b^k \\ &= a^{m+1} + \sum_{k=1}^{m} \binom{m}{k} a^{m+1-k} b^k \end{aligned}$$

and

$$\begin{aligned} b(a+b)^m &= \sum_{j=0}^{m} \binom{m}{j} a^{m-j} b^{j+1} \\ &= \sum_{k=1}^{m} \binom{m}{k-1} a^{m+1-k} b^k + b^{m+1}. \end{aligned}$$

Upon adding these expressions, we obtain

$$\begin{aligned} (a+b)^{m+1} &= a^{m+1} + \sum_{k=1}^{m} \left[\binom{m}{k} + \binom{m}{k-1} \right] a^{m+1-k} b^k + b^{m+1} \\ &= \sum_{k=0}^{m+1} \binom{m+1}{k} a^{m+1-k} b^k, \end{aligned}$$

which is the formula in the case $n = m+1$. This establishes the binomial theorem by induction. □

Example 2. (a) Derive Newton's identity

$$\binom{n}{k}\binom{k}{r} = \binom{n}{r}\binom{n-r}{k-r} \qquad n \geq k \geq r \geq 0.$$

(b) Use part (a) to express $\binom{n}{k}$ in terms of its predecessor:

$$\binom{n}{k} = \frac{n-k+1}{k}\binom{n}{k-1} \qquad n \geq k \geq 1.$$

Example 3. The Catalan numbers, defined by

$$C_n = \frac{1}{n+1}\binom{2n}{n} = \frac{(2n)!}{n!(n+1)!} \qquad n = 0, 1, 2, \ldots$$

form the sequence $1, 1, 2, 5, 14, 42, 132, 429, 1430, 4862, \ldots$. They first appeared in 1838 when Eugène Catalan (1814-1894) showed that there are C_n ways of parenthesizing a nonassociative product of $n+1$ factors. [For instance, when $n = 3$ there are five ways: $((ab)c)d$, $(a(bc))d$, $a((bc)d)$, $a(b(cd))$, $(ab)(ac)$.] For $n \geq 1$, prove that C_n can be given inductively by

$$C_n = \frac{2(2n-1)}{n+1} C_{n-1}.$$

Chapter 2

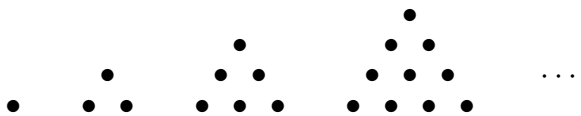
Divisibility Theory in the Integers

2.1 Early Number Theory

Example 1. Each of the numbers

$$1 = 1, 3 = 1 + 2, 6 = 1 + 2 + 3, 10 = 1 + 2 + 3 + 4, \ldots$$

represents the number of dots that can be arranged evenly in an equilateral triangle:



This led the ancient Greeks to call a number triangular if it is the sum of consecutive integers, beginning with 1. Prove the following facts concerning triangular numbers:

(a) A number is triangular if and only if it is of the form $n(n+1)/2$ for some $n \geq 1$. (Pythagoras, circa 550 B.C.)

(b) The integer n is a triangular number if and only if $8n + 1$ is a perfect square. (Plutarch, circa 100 A.D.)

(c) The sum of any two consecutive triangular numbers is a perfect square. (Nicomachus, circa 100 A.D.)

(d) If n is a triangular number, then so are $9n + 1$, $25n + 3$, and $49n + 6$. (Euler, 1775)

Example 2. If t_n denotes the nth triangular number, prove that in terms of the binomial coefficients,

$$t_n = \binom{n+1}{2} \qquad n \geq 1.$$

Example 3. Derive the following formula for the sum of triangular numbers, attributed to the Hindu mathematician Aryabhata (circa 500 A.D.):

$$t_1 + t_2 + t_3 + \cdots + t_n = \frac{n(n+1)(n+2)}{6} \qquad n \geq 1.$$

[*Hint:* Group the terms on the left-hand side in pairs, noting the identity $t_{k-1} + t_k = k^2$.]

2.2 The Division Algorithm

Theorem 2.2.1 (Division Algorithm)**.** *Given integers a and b, with $b > 0$, there exist unique integers q and r satisfying*

$$a = qb + r \qquad 0 \leq r < b.$$

The integers q and r are called, respectively, the quotient and remainder in the division of a by b.

Proof. We begin by proving that the set

$$S = \{a - xb \mid x \text{ an integer; } a - xb \geq 0\}$$

is nonempty. To do this, it suffices to exhibit a value of x making $a - xb$ nonnegative. Because the integer $b \geq 1$, we have $|a|b \geq |a|$, and so

$$a - (-|a|)b = a + |a|b \geq a + |a| \geq 0.$$

For the choice $x = -|a|$, then, $a - xb$ lies in S. This paves the way for an application of the Well-Ordering Principle (Chapter 1), from which we infer that the set S contains a smallest integer; call it r. By the definition of S, there exists an integer q satisfying

$$r = a - qb \qquad 0 \leq r.$$

We argue that $r < b$. If this were not the case, then $r \geq b$ and

$$a - (q + 1)b = (a - qb) - b = r - b \geq 0.$$

The implication is that the integer $a - (q + 1)b$ has the proper form to belong to the set S. But $a - (q + 1)b = r - b < r$, leading to a contradiction of the choice of r as the smallest member of S. Hence, $r < b$.

Next we turn to the task of showing the uniqueness of q and r. Suppose that a has two representations of the desired form, say,

$$a = qb + r = q'b + r'$$

where $0 \leq r < b$, $0 \leq r' < b$. Then $r' - r = b(q - q')$ and, owing to the fact that the absolute value of a product is equal to the product of the absolute values,

$$|r' - r| = b|q - q'|.$$

Upon adding the two inequalities $-b < -r \leq 0$ and $0 \leq r' < b$, we obtain $-b < r' - r < b$ or, in equivalent terms, $|r' - r| < b$. Thus, $b|q - q'| < b$, which yields

$$0 \leq |q - q'| < 1.$$

Because $|q - q'|$ is a nonnegative integer, the only possibility is that $|q - q'| = 0$, whence $q = q'$; this, in turn, gives $r = r'$, ending the proof. □

Example 1. Prove that if a and b are integers, with $b > 0$, then there exist unique integers q and r satisfying $a = qb + r$, where $2b \leq r < 3b$.

Corollary 2.2.1. *If a and b are integers, with $b \neq 0$, then there exist unique integers q and r such that*

$$a = qb + r \qquad 0 \leq r < |b|.$$

Proof. It is enough to consider the case in which b is negative. Then $|b| > 0$, and Theorem 2.2.1 produces unique integers q' and r for which

$$a = q'|b| + r \qquad 0 \leq r < |b|$$

Noting that $|b| = -b$, we may take $q = -q'$ to arrive at $a = qb + r$, with $0 \leq r < |b|$. □

Example 2. Illustrate the Division Algorithm by taking $b = -7$ for the choices of $a = 1, -2, 61$, and -59.

Example 3. Use the Division Algorithm to establish the following:

(a) The square of any integer is of the form $4k + 1$.

(b) The square of any odd integer is either of the form $8k + 1$.

Example 4. Use the Division Algorithm to establish the following:

(a) The square of any integer is either of the form $3k$ or $3k + 1$.

(b) The cube of any integer has one of the forms: $9k$, $9k + 1$, or $9k + 8$.

(c) The fourth power of any integer is either of the form $5k$ or $5k + 1$.

Example 5. Show that the expression $a(a^2+2)/3$ is an integer for all $a \geq 1$.

2.3 The Greatest Common Divisor

Definition 2.3.1. An integer b is said to be divisible by an integer $a \neq 0$, in symbols $a \mid b$, if there exists some integer c such that $b = ac$. We write $a \nmid b$ to indicate that b is not divisible by a.

Theorem 2.3.1. *For integers a, b, c, the following hold:*

(a) $a \mid 0$, $1 \mid a$, $a \mid a$.

(b) $a \mid 1$ *if and only if* $a = \pm 1$.

(c) *If* $a \mid b$ *and* $c \mid d$, *then* $ac \mid bd$.

(d) *If* $a \mid b$ *and* $b \mid c$, *then* $a \mid c$.

(e) $a \mid b$ *and* $b \mid a$ *if and only if* $a = \pm b$.

(f) *If* $a \mid b$ *and* $b \neq 0$, *then* $|a| \leq |b|$.

(g) *If* $a \mid b$ *and* $a \mid c$, *then* $a \mid (bx + cy)$ *for arbitrary integers* x *and* y.

Proof. For (a), $a \mid 0$ is the same as saying that $0 = ac$ for some integer c, and we can simply take $c = 0$. Similarly, we can take $c = a$ for $1 \mid a$ and $c = 1$ for $a \mid a$.

For (b), if $a \mid 1$ then $1 = ac$ for some integer $c = 1/a$, implying $a = \pm 1$. Conversely, if $a = \pm 1$ then $1 = ac$ is true for the integer $c = \pm 1$, implying $a \mid 1$.

For (c), the relations $a \mid b$ and $c \mid d$ ensure that $b = ar$ and $d = cs$ for suitable integers r and s. Thus $bd = (ac)rs$, where rs is an integer, i.e., $ac \mid bd$.

For (d), the relations $a \mid b$ and $b \mid c$ ensure that $b = ar$ and $c = bs$ for suitable integers r and s. Thus $c = (a)rs$, where rs is an integer, i.e., $a \mid c$.

For (e), if $a \mid b$ and $b \mid a$, then $b = ar$ and $a = bs$ for suitable integers r and s. Thus $a = (ar)s$, i.e., $1 = rs$. This implies that $r = s = \pm 1$, and so $a = \pm b$. Conversely, if $a = \pm b$, then $b = ar$ and $a = bs$ is true for $\pm 1 = r = s$, implying $a \mid b$ and $b \mid a$.

As for (f), if $a \mid b$, then there exists an integer c such that $b = ac$; also, $b \neq 0$ implies that $c \neq 0$. Upon taking absolute values, we get $|b| = |ac| = |a||c|$. Because $c \neq 0$, it follows that $|c| \geq 1$, whence $|b| = |a||c| \geq |a|$.

Finally, as regards (g), the relations $a \mid b$ and $a \mid c$ ensure that $b = ar$ and $c = as$ for suitable integers r and s. But then whatever the choice of x and y,

$$bx + cy = arx + asy = a(rx + sy).$$

Because $rx + sy$ is an integer, this says that $a \mid (bx + cy)$, as desired. □

Example 1. If $a \mid b$, show that $(-a) \mid b$, $a \mid (-b)$, and $(-a) \mid (-b)$.

Definition 2.3.2. Let a and b be given integers, with at least one of them different from zero. The greatest common divisor of a and b, denoted by $\gcd(a, d)$, is the positive integer d satisfying the following:

(a) $d \mid a$ and $d \mid b$.

(b) If $c \mid a$ and $c \mid b$, then $c \leq d$.

Example 2. Find $\gcd(-12, 30)$, $\gcd(-5, 5)$, $\gcd(8, 17)$, and $\gcd(-8, -36)$.

Example 3. For a nonzero integer a, show that $\gcd(a, 0) = |a|$, $\gcd(a, a) = |a|$, and $\gcd(a, 1) = 1$.

Theorem 2.3.2. *Given integers a and b, not both of which are zero, there exist integers x and y such that*

$$\gcd(a, b) = ax + by.$$

Proof. Notice first that S is not empty. For example, if $a \neq 0$, then the integer $|a| = au + b \cdot 0$ lies in S, where we choose $u = 1$ or $u = -1$ according as a is positive or negative. By virtue of the Well-Ordering Principle, S must contain a smallest element d. Thus, from the very definition of S, there exist integers x and y for which $d = ax + by$. We claim that $d = \gcd(a, b)$.

Taking stock of the Division Algorithm, we can obtain integers q and r such that $a = qd + r$, where $0 \leq r < d$. Then r can be written in the form

$$\begin{aligned} r = a - qd &= a - q(ax + by) \\ &= a(1 - qx) + b(-qy). \end{aligned}$$

If r were positive, then this representation would imply that r is a member of S, contradicting the fact that d is the least integer in S (recall that $r < d$). Therefore, $r = 0$, and so $a = qd$, or equivalently $d \mid a$. By similar reasoning, $d \mid b$, the effect of which is to make d a common divisor of a and b.

Now if c is an arbitrary positive common divisor of the integers a and b, then part (g) of Theorem 2.3.1 allows us to conclude that $c \mid (ax + by)$; that is, $c \mid d$. By part (f) of the same theorem, $c = |c| \leq |d| = d$, so that d is greater than every positive common divisor of a and b. Piecing the bits of information together, we see that $d = \gcd(a, d)$. □

Example 4. If $a \mid bc$, show that $a \mid \gcd(a, b) \gcd(a, c)$.

Corollary 2.3.1. *If a and b are given integers, not both zero, then the set*

$$T = \{ax + by \mid x, y \text{ are integers}\}$$

is precisely the set of all multiples of $d = \gcd(a, d)$.

Proof. Because $d \mid a$ and $d \mid b$, we know that $d \mid (ax + by)$ for all integers x, y. Thus, every member of T is a multiple of d. Conversely, d may be written as $d = ax_0 + by_0$ for suitable integers x_0 and y_0, so that any multiple nd of d is of the form

$$nd = n(ax_0 + by_0) = a(nx_0) + b(ny_0).$$

Hence, nd is a linear combination of a and b, and, by definition, lies in T. □

Definition 2.3.3. Two integers a and b, not both of which are zero, are said to be relatively prime whenever $\gcd(a, b) = 1$.

Theorem 2.3.3. *Let a and b be integers, not both zero. Then a and b are relatively prime if and only if there exist integers x and y such that $1 = ax+by$.*

Proof. If a and b are relatively prime so that $\gcd(a, b) = 1$, then Theorem 2.3.2 guarantees the existence of integers x and y satisfying $1 = ax + by$. As for the converse, suppose that $1 = ax + by$ for some choice of x and y, and that $d = \gcd(a, b)$. Because $d \mid a$ and $d \mid b$, Theorem 2.3.1 yields $d \mid (ax + by)$, or $d \mid 1$. Inasmuch as d is a positive integer, this last divisibility condition forces d to equal 1 (part (b) of Theorem 2.3.1 plays a role here), and the desired conclusion follows. □

Corollary 2.3.2. *If $\gcd(a, b) = d$, then $\gcd(a/d, b/d) = 1$.*

Proof. Before starting with the proof proper, we should observe that although a/d and b/d have the appearance of fractions, in fact, they are integers because d is a divisor of both a and of b. Now, knowing that $\gcd(a, d) = d$, it is possible to find integers x and y such that $d = ax + by$. Upon dividing each side of this equation by d, we obtain the expression

$$1 = \left(\frac{a}{d}\right) x + \left(\frac{b}{d}\right) y.$$

Because a/d and b/d are integers, an appeal to the theorem is legitimate. The conclusion is that a/d and b/d are relatively prime. □

Corollary 2.3.3. *If $a \mid c$ and $b \mid c$, with $\gcd(a, b) = 1$, then $ab \mid c$.*

Proof. Inasmuch as $a \mid c$ and $b \mid c$, integers r and s can be found such that $c = ar = bs$. Now the relation $\gcd(a, b) = 1$ allows us to write $1 = ax + by$ for some choice of integers x and y. Multiplying the last equation by c, it appears that

$$c = c \cdot 1 = c(ax + by) = acx + bcy.$$

If the appropriate substitutions are now made on the right-hand side, then

$$c = a(bs)x + b(ar)y = ab(sx + ry),$$

or, as a divisibility statement, $ab \mid c$. □

Example 5. Prove: The product of any three consecutive integers is divisible by 6; the product of any four consecutive integers is divisible by 24; the product of any five consecutive integers is divisible by 120.

Theorem 2.3.4 (Euclid's Lemma)**.** *If $a \mid bc$, with $\gcd(a, b) = 1$, then $a \mid c$.*

Proof. We start again from Theorem 2.3.2, writing $1 = ax + by$, where x and y are integers. Multiplication of this equation by c produces

$$c = 1 \cdot c = (ax + by)c = acx + bcy.$$

Because $a \mid ac$ and $a \mid bc$, it follows that $a \mid (acx + bcy)$, which can be recast as $a \mid c$. □

Theorem 2.3.5. *Let a, b be integers, not both zero. For a positive integer d, $d = \gcd(a, b)$ if and only if*

(a) *$d \mid a$ and $d \mid b$.*

(b) *Whenever $c \mid a$ and $c \mid b$, then $c \mid d$.*

Proof. To begin, suppose that $d = \gcd(a, b)$. Certainly, $d \mid a$ and $d \mid b$, so that (a) holds. In light of Theorem 2.3.2, d is expressible as $d = ax + by$ for some integers x, y. Thus, if $c \mid a$ and $c \mid b$, then $c \mid (ax + by)$, or rather $c \mid d$. In short, condition (b) holds. Conversely, let d be any positive integer satisfying the stated conditions. Given any common divisor c of a and b, we have $c \mid d$ from hypothesis (b). The implication is that $d \geq c$, and consequently d is the greatest common divisor of a and b. □

Example 6. (a) Prove that if $d \mid n$, then $2^d - 1 \mid 2^n - 1$.

(b) Verify that $2^{35} - 1$ is divisible by 31 and 127.

2.4 The Euclidean Algorithm

Remark 1. The Euclidean Algorithm may be described as follows: let a and b be two integers whose greatest common divisor is desired. Because $\gcd(|a|, |b|) = \gcd(a, b)$, there is no harm in assuming that $a \geq b > 0$. The first step is to apply the Division Algorithm to a and b to get

$$a = q_1 b + r_1 \qquad 0 \leq r_1 < b.$$

If it happens that $r_1 = 0$, then $b \mid a$ and $\gcd(a, b) = b$. When $r_1 \neq 0$, divide b by r_1 to produce integers q_2 and r_2 satisfying

$$b = q_2 r_1 + r_2 \qquad 0 \leq r_2 < r_1.$$

If $r_2 = 0$, then we stop; otherwise, proceed as before to obtain

$$r_1 = q_3 r_2 + r_3 \qquad 0 \leq r_3 < r_2.$$

This division process continues until some zero remainder appears, say, at the $(n+1)$th stage where r_{n-1} is divided by r_n (a zero remainder occurs sooner or later because the decreasing sequence $b > r_1 > r_2 > \cdots \geq 0$ cannot contain more than b integers).

***Lemma* 2.4.1:** If $a = qb + r$, then $\gcd(a, b) = \gcd(b, r)$.

Proof. If $d = \gcd(a, b)$, then the relations $d \mid a$ and $d \mid b$ together imply that $d \mid (a - qb)$, or $d \mid r$. Thus, d is a common divisor of both b and r. On the other hand, if c is an arbitrary common divisor of b and r, then $c \mid (qb + r)$, whence $c \mid a$. This makes c a common divisor of a and b, so that $c \leq d$. It now follows from the definition of $\gcd(b, r)$ that $d = \gcd(b, r)$. □

Example 1. Calculate $\gcd(12378, 3054)$.

Example 2. Use the Euclidean Algorithm to obtain integers x and y satisfying the following:

(a) $\gcd(56, 72) = 56x + 72y$.

(b) $\gcd(24, 138) = 24x + 138y$.

(c) $\gcd(119, 272) = 119x + 272y$.

(d) $\gcd(1769, 2378) = 1769x + 2378y$.

Theorem 2.4.1. *If $k > 0$, then* $\gcd(ka, kb) = k \gcd(a, b)$.

Proof. If each of the equations appearing in the Euclidean Algorithm for a and b is multiplied by k, we obtain

$$\begin{aligned} ak &= q_1(bk) + r_1k \qquad 0 < r_1k < bk \\ bk &= q_2(r_1k) + r_2k \qquad 0 < r_2k < r_1k \\ &\vdots \\ r_{n-2}k &= q_n(r_{n-1}k) + r_nk \qquad 0 < r_nk < r_{n-1}k \\ r_{n-1}k &= q_{n+1}(r_nk) + 0. \end{aligned}$$

But this is clearly the Euclidean Algorithm applied to the integers ak and bk, so that their greatest common divisor is the last nonzero remainder r_nk; that is,

$$\gcd(ka, kb) = r_nk = k \gcd(a, b),$$

as stated in the theorem. □

Corollary 2.4.1. *For any integer $k \neq 0$,* $\gcd(ka, kb) = |k| \gcd(a, b)$.

Proof. It suffices to consider the case in which $k < 0$. Then $-k = |k| > 0$ and, by Theorem 2.4.1,

$$\begin{aligned} \gcd(ak, bk) &= \gcd(-ak, -bk) \\ &= \gcd(a|k|, b|k|) \\ &= |k| \gcd(a, b). \end{aligned}$$

□

Example 3. Prove that if d is a common divisor of a and b, then $d = \gcd(a, b)$ if and only if $\gcd(a/d, b/d) = 1$.

Definition 2.4.1. The least common multiple of two nonzero integers a and b, denoted by $\text{lcm}(a, b)$, is the positive integer m satisfying the following:

(a) $a \mid m$ and $b \mid m$.

(b) If $a \mid c$ and $b \mid c$, with $c > 0$, then $m \leq c$.

Theorem 2.4.2. *For positive integers a and b*

$$\gcd(a, b)\,\text{lcm}(a, b) = ab.$$

Proof. To begin, put $d = \gcd(a, b)$ and write $a = dr$, $b = ds$ for integers r and s. If $m = ab/d$, then $m = as = rb$, the effect of which is to make m a (positive) common multiple of a and b.

Now let c be any positive integer that is a common multiple of a and b; say, for definiteness, $c = au = bv$. As we know, there exist integers x and y satisfying $d = ax + by$. In consequence,

$$\frac{c}{m} = \frac{cd}{ab} = \frac{c(ax + by)}{ab} = \left(\frac{c}{b}\right) x + \left(\frac{c}{a}\right) y = vx + uy.$$

This equation states that $m \mid c$, allowing us to conclude that $m \leq c$. Thus, in accordance with Definition 2.4.1, $m = \text{lcm}(a, b)$; that is,

$$\text{lcm}(a, b) = \frac{ab}{d} = \frac{ab}{\gcd(a, b)},$$

which is what we started out to prove. □

Corollary 2.4.2. *For any choice of positive integers a and b,* $\text{lcm}(a, b) = ab$ *if and only if* $\gcd(a, b) = 1$.

Example 4. Prove that the greatest common divisor of two positive integers divides their least common multiple.

2.5 The Diophantine Equation $ax + by = c$

Theorem 2.5.1. *The linear Diophantine equation $ax + by = c$ has a solution if and only if $d \mid c$, where $d = \gcd(a, b)$. If x_0, y_0 is any particular solution of this equation, then all other solutions are given by*

$$x = x_0 + \left(\frac{b}{d}\right) t \qquad y = y_0 - \left(\frac{a}{d}\right) t$$

where t is an arbitrary integer.

Proof. We know that there are integers r and s for which $a = dr$ and $b = ds$. If a solution of $ax + by = c$ exists, so that $ax_0 + by_0 = c$ for suitable x_0 and y_0, then

$$c = ax_0 + by_0 = c = drx_0 + dsy_0 = d(rx_0 + sy_0),$$

which simply says that $d \mid c$. Conversely, assume that $d \mid c$, say $c = dt$. Using Theorem 2.3.2, integers x_0 and y_0 can be found satisfying $d = ax_0 + by_0$. When this relation is multiplied by t, we get

$$c = dt = (ax_0 + by_0)t = a(tx_0) + b(ty_0).$$

Hence, the Diophantine equation $ax + by = c$ has $x = tx_0$ and $y = ty_0$ as a particular solution.

To establish the second assertion of the theorem, let us suppose that a solution x_0, y_0 of the given equation is known. If x', y' is any other solution, then

$$ax_0 + by_0 = c = ax' + by',$$

which is equivalent to

$$a(x' - x_0) = b(y_0 - y').$$

By Corollary 2.3.2, there exist relatively prime integers r and s such that $a = dr$, $b = ds$. Substituting these values into the last-written equation and canceling the common factor d, we find that

$$r(x' - x_0) = s(y_0 - y').$$

The situation is now this: $r \mid s(y_0 - y')$, with $\gcd(r, s) = 1$. Using Euclid's lemma, it must be the case that $r \mid (y_0 - y')$; or, in other words, $y_0 - y' = rt$ for some integer t. Substituting, we obtain

$$x' - x_0 = st.$$

This leads us to the formulas

$$x' = x_0 + st = x_0 + \left(\frac{b}{d}\right) t$$
$$y' = y_0 - rt = y_0 - \left(\frac{a}{d}\right) t.$$

It is easy to see that these values satisfy the Diophantine equation, regardless of the choice of the integer t; for

$$\begin{aligned} ax' + by' &= a\left[x_0 + \left(\frac{b}{d}\right) t\right] + b\left[y_0 - \left(\frac{a}{d}\right) t\right] \\ &= (ax_0 + by_0) + \left(\frac{ab}{d} - \frac{ab}{d}\right) t \\ &= c + 0 \cdot t \\ &= c. \end{aligned}$$

Thus, there are an infinite number of solutions of the given equation, one for each value of t. □

Example 1. Consider the linear Diophantine equation

$$172x + 20y = 1000.$$

Find the solutions in the positive integers.

Corollary 2.5.1. *If* $\gcd(a, b) = 1$ *and if* x_0, y_0 *is a particular solution of the linear Diophantine equation* $ax + by = c$, *then all solutions are given by*

$$x = x_0 + bt \qquad y = y_0 - at$$

for integral values of t.

Example 2. A customer bought a dozen pieces of fruit, apples and oranges, for \$1.32. If an apple costs 3 cents more than an orange and more apples than oranges were purchased, how many pieces of each kind were bought?

Example 3. When Mr. Smith cashed a check at his bank, the teller mistook the number of cents for the number of dollars and vice versa. Unaware of this, Mr. Smith spent 68 cents and then noticed to his surprise that he had twice the amount of the original check. Determine the smallest value for which the check could have been written.

Chapter 3

Primes and Their Distribution

3.1 The Fundamental Theorem of Arithmetic

Definition 3.1.1. An integer $p > 1$ is called a prime number, or simply a prime, if its only positive divisors are 1 and p. An integer greater than 1 that is not a prime is termed composite.

Example 1. If $p \geq 5$ is a prime number, show that $p^2 + 2$ is composite.

Theorem 3.1.1. *If p is a prime and $p \mid ab$, then $p \mid a$ or $p \mid b$.*

Proof. If $p \mid a$, then we need go no further, so let us assume that $p \nmid a$. Because the only positive divisors of p are 1 and p itself, this implies that $\gcd(p, a) = 1$. (In general, $\gcd(p, a) = p$ or $\gcd(p, a) = 1$ according as $p \mid a$ or $p \nmid a$.) Hence, citing Euclid's lemma, we get $p \mid b$. □

Corollary 3.1.1. *If p is a prime and $p \mid a_1 a_2 \cdots a_n$, then $p \mid a_k$ for some k, where $1 \leq k \leq n$.*

Proof. We proceed by induction on n, the number of factors. When $n = 1$, the stated conclusion obviously holds; whereas when $n = 2$, the result is the content of Theorem 3.1.1. Suppose, as the induction hypothesis, that $n > 2$ and that whenever p divides a product of less than n factors, it divides at least one of the factors. Now $p \mid a_1 a_2 \cdots a_n$. From Theorem 3.1.1, either $p \mid a_n$ or $p \mid a_1 a_2 \cdots a_{n-1}$. If $p \mid a_n$, then are through. As regards the case where $p \mid a_1 a_2 \cdots a_{n-1}$, the induction hypothesis ensures that $p \mid a_k$ for some choice of k, with $1 \leq k \leq n-1$. In any event, p divides one of the integers $a_1, a_2, \ldots, a_n$. □

Example 2. (a) Given that p is a prime and $p \mid a^n$, prove that $p^n \mid a^n$.

(b) If $\gcd(a, b) = p$, a prime, what are the possible values of $\gcd(a^2, b^2)$, $\gcd(a^2, b)$ and $\gcd(a^3, b^2)$?

Corollary 3.1.2. *If $p, q_1, q_2, \ldots, q_n$ are all primes and $p \mid q_1 q_2 \cdots q_n$, then $p = q_k$ for some k, where $1 \leq k \leq n$.*

Proof. By virtue of Corollary 3.1.1, we know that $p \mid q_k$ for some k, with $1 \leq k \leq n$. Being a prime, q_k is not divisible by any positive integer other than 1 or q_k itself. Because $p > 1$, we are forced to conclude that $p = q_k$. □

Theorem 3.1.2 (Fundamental Theorem of Arithmetic)**.** *Every positive integer $n > 1$ is either a prime or a product of primes; this representation is unique, apart from the order in which the factors occur.*

Proof. Either n is a prime or it is composite; in the former case, there is nothing more to prove. If n is composite, then there exists an integer d satisfying $d \mid n$ and $1 < d < n$. Among all such integers d, choose p_1 to be the smallest (this is possible by the Well-Ordering Principle). Then p_1 must be a prime number. Otherwise it too would have a divisor q with $1 < q < p_1$; but then $q \mid p_1$ and $p_1 \mid n$ imply that $q \mid n$, which contradicts the choice of p_1 as the smallest positive divisor, not equal to 1, of n.

We therefore may write $n = p_1 n_1$, where p_1 is prime and $1 < n_1 < n$. If n_1 happens to be a prime, then we have our representation. In the contrary

case, the argument is repeated to produce a second prime number p_2 such that $n_1 = p_2 n_2$; that is,

$$n = p_1 p_2 n_2 \qquad 1 < n_2 < n_1.$$

If n_2 is a prime, then it is not necessary to go further. Otherwise, write $n_2 = p_3 n_3$, with p_3 a prime:

$$n = p_2 p_2 p_3 n_3 \qquad 1 < n_3 < n_2.$$

The decreasing sequence

$$n > n_1 > n_2 > \cdots > 1$$

cannot continue indefinitely, so that after a finite number of steps n_{k-1} is a prime, call it, p_k. This leads to the prime factorization

$$n = p_1 p_2 \cdots p_k.$$

To establish the second part of the proof—the uniqueness of the prime factorization—let us suppose that the integer n can be represented as a product of primes in two ways; say,

$$n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s \qquad r \leq s$$

where the p_i and q_j are all primes, written in increasing magnitude so that

$$p_1 \leq p_2 \leq \cdots \leq p_r \qquad q_1 \leq q_2 \leq \cdots \leq q_s.$$

Because $p_1 \mid q_1 q_2 \cdots q_s$, Corollary 3.1.2 of Theorem 3.1.1 tells us that $p_1 = q_k$ for some k; but then $p_1 \geq q_1$. Similar reasoning gives $q_1 \geq p_1$, whence $p_1 = q_1$. We may cancel this common factor and obtain

$$p_2 p_3 \cdots p_r = q_2 q_2 \cdots q_s.$$

Now repeat this process to get $p_2 = q_2$ and, in turn,

$$p_3 p_4 \cdots p_r = q_3 q_4 \cdots q_s.$$

Continue in this fashion. If the inequality $r < s$ were to hold, we would eventually arrive at

$$1 = q_{r+1} q_{r+2} \cdots q_s,$$

which is absurd, because each $q_j > 1$. Hence, $r = s$ and

$$p_1 = q_1 \qquad p_2 = q_2, \ldots, p_r = q_r$$

making the two factorizations of n identical. The proof is now complete. □

Example 3. Find all primes that divide 50!.

Corollary 3.1.3. *Any positive integer $n > 1$ can be written uniquely in a canonical form*

$$n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$$

where, for $i = 1, 2, \ldots, r$, each k_i is a positive integer and each p_i is a prime, with $p_1 < p_2 < \cdots p_r$.

Example 4. Prove that a positive integer $a > 1$ is a square if and only if in the canonical form of a all the exponents of the primes are even integers.

Theorem 3.1.3 (Pythagoras)**.** *The number $\sqrt{2}$ is irrational.*

Proof. Suppose, to the contrary, that $\sqrt{2}$ is a rational number, say, $\sqrt{2} = a/b$, where a and b are both integers with $\gcd(a, b) = 1$. Squaring, we get $a^2 = 2b^2$, so that $b \mid a^2$. If $b > 1$, then the Fundamental Theorem of Arithmetic guarantees the existence of a prime p such that $p \mid b$. It follows that $p \mid a^2$ and, by Theorem 3.1.1, that $p \mid a$; hence, $\gcd(a, b) \geq p$. We therefore arrive at a contradiction, unless $b = 1$. But if this happens, then $a^2 = 2$, which is impossible. Our supposition that $\sqrt{2}$ is a rational number is untenable, and so $\sqrt{2}$ must be rational. □

3.2 The Sieve of Eratosthenes

Example 1. Determine whether 509 is a prime number.

Example 2. Determine the canonical form of 2093.

Example 3. Find all primes not exceeding 100.

Theorem 3.2.1 (Euclid)**.** *There is an infinite number of primes.*

Proof. Euclid's proof is by contradiction. Let $p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 7, \ldots$ be the primes in ascending order, and suppose that there is a last prime, called p_n. Now consider the positive integer

$$P = p_1 p_2 \cdots p_n + 1.$$

Because $P > 1$, we may put Theorem 3.1.2 to work once again and conclude that P is divisible by some prime p. But $p_1, p_2, \ldots, p_n$ are the only prime numbers, so that p must be equal to one of $p_1, p_2, \ldots, p_n$. Combining the divisibility relation $p \mid p_1 p_2 \cdots p_n$ with $p \mid P$, we arrive at $p \mid P - p_1 p_2 \cdots p_n$ or, equivalently, $p \mid 1$. The only positive divisor of the integer 1 is 1 itself and, because $p > 1$, a contradiction arises. Thus, no finite list of primes is complete, whence the number of primes is infinite. □

Theorem 3.2.2. *If p_n is the nth prime number, then $p_n \leq 2^{2^{n-1}}$.*

Proof. Let us proceed by induction on n, the asserted inequality being clearly true when $n = 1$. As the hypothesis of the induction, we assume that $n > 1$ and that the result holds for all integers up to n. Then

$$\begin{aligned} p_{n+1} &\leq p_1 p_2 \cdots p_n + 1 \\ &\leq 2 \cdot 2^2 \cdots 2^{2^{n-1}} + 1 = 2^{1+2+2^2+\cdots+2^{n-1}} + 1. \end{aligned}$$

Recalling the identity $1 + 2 + 2^2 + \cdots + 2^{n-1} = 2^n - 1$, we obtain

$$p_{n+1} \leq 2^{2^{n-1}} + 1.$$

However, $1 \leq 2^{2^{n-1}}$ for all n; whence

$$\begin{aligned} p_{n+1} &\leq 2^{2^{n-1}} + 2^{2^{n-1}} \\ &= 2 \cdot 2^{2^{n-1}} = 2^{2^n} \end{aligned}$$

completing the induction step, and the argument. □

Corollary 3.2.1. *For $n \geq 1$, there are at least $n + 1$ primes less than 2^{2^n}.*

Proof. From the theorem, we know that $p_1, p_2, \ldots, p_{n+1}$ are all less than 2^{2^n}. □

Example 4. Assuming that p_n is the nth prime number, establish each of the following statements:

(a) $p_n > 2n - 1$ for $n \geq 5$.

(b) None of the integers $P_n = p_1 p_2 \cdots p_n + 1$ is a perfect square.

(c) The sum

$$\frac{1}{p_1} + \frac{1}{p_2} + \cdots + \frac{1}{p_n}$$

is never an integer.

3.3 The Goldbach Conjecture

Example 1. (a) If 1 is added to a product of twin primes, prove that a perfect square is always obtained.

(b) Show that the sum of twin primes p and $p+2$ is divisible by 12, provided that $p > 3$.

Example 2. Prove that the Goldbach conjecture that every even integer greater than 2 is the sum of two primes is equivalent to the statement that every integer greater than 5 is the sum of three primes.

***Lemma* 3.3.1:** The product of two or more integers of the form $4n + 1$ is of the same form.

Proof. It is sufficient to consider the product of just two integers. Let us take $k = 4n + 1$ and $k' = 4m + 1$. Multiplying these together, we obtain

$$\begin{aligned} kk' &= (4n + 1)(4m + 1) \\ &= 16nm + 4n + 4m + 1 = 4(4nm + n + m) + 1, \end{aligned}$$

which is of the desired form. □

Theorem 3.3.1. *There are an infinite number of primes of the form $n + 3$.*

Proof. In anticipation of a contradiction, let us assume that there exist only finitely many primes of the form $4n + 3$; call them $q_1, q_2, \ldots, q_s$. Consider the positive integer

$$N = 4q_1q_2 \cdots q_s - 1 = 4(q_1q_2 \cdots q_s - 1) + 3$$

and let $N = r_1r_2 \cdots r_t$ be its prime factorization. Because N is an odd integer, we have $r_k \neq 2$ for all k, so that each r_k is either of the form $4n + 1$ or $4n + 3$. By the lemma, the product of any number of primes of the form $4n+1$ is again an integer of this type. For N to take the form $4n + 3$, as it clearly does, N must contain at least one prime factor r_i of the form $4n + 3$. But r_i cannot be found among the listing $q_1, q_2, \ldots, q_s$, for this would lead to the contradiction that $r_i \mid 1$. The only possible conclusion is that there are infinitely many primes of the form $4n + 3$. □

Example 3. Show that there are infinitely many primes of the form $6n + 5$.

Theorem 3.3.2 (Dirichlet)**.** *If a and b are relatively prime positive integers, then the arithmetic progression*

$$a, a + b, a + 2b, a + 3b, \ldots$$

contains infinitely many primes.

Theorem 3.3.3. *If all the $n > 2$ of the arithmetic progression*

$$p, p + d, p + 2d, \ldots, p + (n - 1)d$$

are prime numbers, then the common difference d is divisible by every prime $q < n$.

Proof. Consider a prime number $q < n$ and assume to the contrary that $q \nmid d$. We claim that the first q terms of the progression

$$p, p + d, p + 2d, \ldots, p + (q - 1)d \tag{1}$$

will leave different remainders, when divided by q. Otherwise there exist integers j and k, with $0 \leq j < k \leq q-1$, such that the numbers $p+jd$ and $p+kd$ yield the same remainder upon division by q. Then q divides their difference $(k-j)d$. But $\gcd(q,d) = 1$, and so Euclid's lemma leads to $q \mid k-j$, which is nonsense in light of the inequality $k - j \leq q - 1$.

Because the q different remainders produced from equation (1) are drawn from the q integers $0, 1, \ldots, q-1$, one of these remainders must be zero. This means that $q \mid p + td$ for some t satisfying $0 \leq t \leq q - 1$. Because of the inequality $q < n \leq p \leq p + td$, we are forced to conclude that $p + td$ is composite. (If p were less than n, one of the terms of the progression would be $p + pd = p(1 + d)$.) With this contradiction, the proof $q \mid d$ is complete. □

Example 4. (a) If p is a prime and $p \nmid b$, prove that in the arithmetic progression

$$a, a + b, a + 2b, a + 3b, \ldots$$

every pth term is divisible by p.

(b) From part (a), conclude that if b is an odd integer, then every other term in the indicated progression is even.

Chapter 4

The Theory of Congruences

4.2 Basic Properties of Congruence

Definition 4.2.1. Let n be a fixed positive integer. Two integers a and b are said to be congruent modulo n, symbolized by

$$a \equiv b \pmod{n}$$

if n divides the different $a - b$; that is, provided that $a - b = kn$ for some integer k.

Remark 1. When $n \nmid (a - b)$, we say that a is incongruent to b modulo n, and in this case we write $a \not\equiv b \pmod{n}$.
Given an integer a, let q and r be its quotient and remainder upon division by n, so that

$$a = qn + r \qquad 0 \leq r < n.$$

Then, by definition of congruence, $a \equiv r \pmod{n}$. Because there are n choices for r, we see that every integer is congruent modulo n to exactly one of the values $0, 1, 2, \ldots, n-1$; in particular, $a \equiv 0 \mod n$ if and only if $n \mid a$. The set of n integers $0, 1, 2, \ldots, n-1$ is called the set of least nonnegative residues modulo n.
In general, a collection of n integers $a_1, a_2, \ldots a_n$ is said to form a complete set of residues (or a complete system of residues) modulo n if every integer is congruent modulo n to one and only one of the a_k. To put it another way, $a_1, a_2, \ldots a_n$ are congruent modulo n to $0, 1, 2, \ldots n-1$, taken in some order.

Theorem 4.2.1. *For arbitrary integers a and b, $a \equiv b \pmod{n}$ if and only if a and b leave the same nonnegative remainder when divided by n.*

Proof. First take $a \equiv b \pmod{n}$, so that $a = b + kn$ for some integer k. Upon division by n, b leaves a certain remainder r; that is, $b = qn + r$, where $0 \leq r < n$. Therefore,

$$a = b + kn = (qn + r) + kn = (q + k)n + r,$$

which indicates that a has the same remainder as b.

On the other hand, suppose we can write $a = q_1 n + r$ and $b = q_2 n + r$, with the same remainder r $(0 \leq r < n)$. Then

$$a - b = (q_1 n + r) - (q_2 n + r) = (q_1 - q_2)n$$

whence $n \mid a - b$. In the language of congruences, we have $a \equiv b \pmod{n}$. □

Example 1. Show that $-56 \equiv -11 \pmod{9}$, and show that $-31 \equiv 11 \pmod{7}$ implies that -31 and 11 have the same remainder when divided by 7.

Theorem 4.2.2. *Let $n > 1$ be fixed and a, b, c, d be arbitrary integers. Then the following properties hold:*

(a) $a \equiv a \pmod{n}$.

(b) *If* $a \equiv b \pmod{n}$, *then* $b \equiv a \pmod{n}$.

(c) *If* $a \equiv b \pmod{n}$ *and* $b \equiv c \pmod{n}$, *then* $a \equiv c \pmod{n}$.

(d) *If* $a \equiv b \pmod{n}$ *and* $c \equiv d \pmod{n}$, *then* $a + c \equiv b + d \pmod{n}$ *and* $ac \equiv bd \pmod{n}$.

(e) *If* $a \equiv b \pmod{n}$, *then* $a + c \equiv b + c \pmod{n}$ *and* $ac \equiv bc \pmod{n}$.

(f) *If* $a \equiv b \pmod{n}$, *then* $a^k \equiv b^k \pmod{n}$ *for any positive integer* k.

Proof. For any integer a, we have $a - a = 0 \cdot n$, so that $a \equiv a \pmod{n}$. Now if $a \equiv b \pmod{n}$, then $a - b = kn$ for some integer k. Hence, $b - a = -(kn) = (-k)n$ and because $-k$ is an integer, this yields property (b).

Property (c) is slightly less obvious: Suppose that $a \equiv b \pmod{n}$ and also $b \equiv c \pmod{n}$. Then there exist integers h and k satisfying $a - b = hn$ and $b - c = kn$. It follows that

$$a - c = (a - b) + (b - c) = hn + kn = (h + k)n,$$

which is $a \equiv c \pmod{n}$ in congruence notation.

In the same vein, if $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then we are assured that $a - b = k_1 n$ and $c - d = k_2 n$ for some choice of k_1 and k_2. Adding these equations, we obtain

$$\begin{aligned}(a + c) - (b + d) &= (a - b) + (c - d) \\ &= k_1 n + k_2 n = (k_1 + k_2)n\end{aligned}$$

or, as a congruence statement, $a + c \equiv b + d \pmod{n}$. As regards the second assertion of property (d), note that

$$ac = (b + k_1 n)(d + k_2 n) = bd + (bk_2 + dk_1 + k_1 k_2 n)n.$$

Because $bk_2 + dk_1 + k_1 k_2 n$ is an integer, this says that $ac - bd$ is divisible by n, whence $ac \equiv bd \pmod{n}$.

The proof of property (e) is covered by (d) and the fact that $c \equiv c \pmod{n}$. Finally, we obtain property (f) by making an induction argument. The statement certainly holds for $k = 1$, and we will assume it is true for some fixed k. From (d), we know that $a \equiv b \pmod{n}$ and $a^k \equiv b^k \pmod{n}$ together imply that $aa^k \equiv bb^k \pmod{n}$, or equivalently $a^{k+1} \equiv b^{k+1} \pmod{n}$. This is the form the statement should take for $k+1$, and so the induction step is complete. □

Example 2. Show that 41 divides $2^{20} - 1$.

Example 3. Find the remainder obtained upon dividing the sum

$$1! + 2! + 3! + 4! + \cdots + 99! + 100!$$

by 12.

Theorem 4.2.3. *If* $ca \equiv cb \pmod{n}$*, then* $a \equiv b \pmod{n/d}$*, where* $d = \gcd(c, n)$*.*

Proof. By hypothesis, we can write

$$c(a - b) = ca - cb = kn$$

for some integer k. Knowing that $\gcd(c, d) = d$, there exist relatively prime integers r and s satisfying $c = dr$, $n = ds$. When these values are substituted in the displayed equation and the common factor d canceled, the net result is

$$r(a - b) = ks.$$

Hence, $s \mid r(a - b)$ and $\gcd(r, s) = 1$. Euclid's lemma yields $s \mid a - b$, which may be recast as $a \equiv b \pmod{s}$; in other words, $a \equiv b \pmod{n/d}$. □

Corollary 4.2.1. *If* $ca \equiv cb \pmod{n}$ *and* $\gcd(c, n) = 1$*, then* $a \equiv b \pmod{n}$*.*

Example 4. Prove that whenever $ab \equiv cd \pmod{n}$ and $b \equiv d \pmod{n}$, with $\gcd(b, n) = 1$, then $a \equiv c \pmod{n}$.

Corollary 4.2.2. $ca \equiv cb \pmod{p}$ *and* $p \nmid c$*, where* p *is a prime number, then* $a \equiv b \pmod{p}$*.*

Proof. The conditions $p \nmid c$ and p a prime imply that $\gcd(c, p) = 1$. □

Example 5. Find equivalent congruences to $33 \equiv 15 \pmod{9}$ and $-35 \equiv 45 \pmod{8}$.

4.3 Binary and Decimal Representations of Integers

Example 1. Calculate $5^{110} \pmod{131}$.

Theorem 4.3.1. *Let $P(x) = \sum_{k=0}^{m} c_k x^k$ be a polynomial function of x with integral coefficients c_k. If $a \equiv b \pmod{n}$, then $P(a) \equiv P(b) \pmod{n}$.*

Proof. Because $a \equiv b \pmod{n}$, part (f) of Theorem 4.2.2 can be applied to give $a^k \equiv b^k \pmod{n}$ for $k = 0, 1, \ldots, m$. Therefore,

$$c_k a^k \equiv c_k b^k \pmod{n}$$

for all such k. Adding these $m + 1$ congruences, we conclude that

$$\sum_{k=0}^{m} c_k a^k \equiv \sum_{k=0}^{m} c_k b^k \pmod{n}$$

or, in different notation, $P(a) \equiv P(b) \pmod{n}$. □

Corollary 4.3.1. *If $a \equiv b \pmod{n}$ and a is a solution of $P(x) \equiv 0 \pmod{n}$, i.e., $P(a) \equiv 0 \pmod{n}$, then b also is a solution.*

Proof. From the last theorem, it is known that $P(a) \equiv P(b) \pmod{n}$. Hence, if a is a solution of $P(x) \equiv 0 \pmod{n}$, then $P(b) \equiv P(a) \equiv 0 \pmod{n}$, making b a solution. □

Theorem 4.3.2. *Let $N = a_m 10^m + a_{m-1} 10^{m-1} + \cdots + a_1 10 + a_0$ be the decimal expansion of the positive integer N, $0 \leq a_k < 10$, and let $T = a_0 - a_1 + a_2 - \cdots + (-1)^m a_m$. Then $11 \mid N$ if and only if $11 \mid T$.*

Proof. As in the proof of Theorem 4.3.1, put $P(x) = \sum_{k=0}^{m} a_k x^k$. Because $10 \equiv -1 \pmod{11}$, we get $P(10) \equiv P(-1) \pmod{11}$. But $P(10) = N$, whereas $P(-1) = a_0 - a_1 + a_2 - \cdots + (-1)^m a_m = T$, so that $N \equiv T \pmod{11}$. The implication is that either both N and T are divisible by 11 or neither is divisible by 11. □

Example 2. Determine whether $N = 1{,}571{,}724$ is divisible by 9 and 11.

Example 3. Show that 2^n divides an integer N if and only if 2^n divides the number made up of the last n digits of N.

4.4 Linear Congruences and the Chinese Remainder Theorem

Definition 4.4.1. An equation of the form $ax \equiv b \pmod{n}$ is called a linear congruence, and by a solution of such an equation we mean an integer x_0 for which $ax_0 \equiv b \pmod{n}$.

Theorem 4.4.1. *The linear congruence $ax \equiv b \pmod{n}$ has a solution if and only if $d \mid b$, where $d = \gcd(a, n)$. If $d \mid b$, then it has d mutually incongruent solutions modulo n.*

Proof. The given congruence is equivalent to the linear Diophantine equation $ax - ny = b$. From Theorem 2.5.1, it is known that the latter equation can be solved if and only if $d \mid b$l moreover, if it is solvable and x_0, y_0 is one specific solution, then any other solution has the form

$$x = x_0 + \frac{n}{d}t \qquad y = y_0 + \frac{a}{d}t$$

for some choice of t.

Among the various integers satisfying the first of these formulas, consider that occur when t takes on the successive values $t = 0, 1, 2, \ldots, d-1$:

$$x_0, x_0 + \frac{n}{d}, x_0 + \frac{2n}{d}, \ldots, x_0 + \frac{(d-1)n}{d}.$$

We claim that these integers are incongruent modulo n, and all other such integers x are congruent to some of them. If it happened that

$$x_0 + \frac{n}{d}t_1 \equiv x_0 + \frac{n}{d}t_2 \pmod{n},$$

where $0 \leq t_1 < t_2 \leq d-1$, then we would have

$$\frac{n}{d}t_1 \equiv \frac{n}{d}t_2 \pmod{n}.$$

Now $\gcd(n/d, n) = n/d$, and therefore by Theorem 4.2.3 the factor n/d could be canceled to arrive at the congruence

$$t_1 \equiv t_2 \pmod{d},$$

which is to say that $d \mid t_2 - t_1$. But this is impossible in view of the inequality $0 < t_2 - t_1 < d$.

It remains to argue that any other solution $x_0 + (n/d)t$ is incongruent

modulo n to one of the d integers listed above. The Division Algorithm permits us to write t as $t = qd + r$, where $0 \leq r \leq d - 1$. Hence

$$\begin{aligned} x_0 + \frac{n}{d}t &= x_0 + \frac{n}{d}(qd + r) \\ &= x_0 + nq + \frac{n}{d}r \\ &\equiv x_0 + \frac{n}{d}r \pmod{n} \end{aligned}$$

with $x_0 + (n/d)r$ being one of our d selected solutions. □

Corollary 4.4.1. *If* $\gcd(a, n) = 1$*, then the linear congruence* $ax \equiv b \pmod{n}$ *has a unique solution modulo* n*.*

Example 1. Solve the linear congruence $18x \equiv 30 \pmod{42}$.

Example 2. Solve the linear congruence $9x \equiv 21 \pmod{30}$.

Theorem 4.4.2 (Chinese Remainder Theorem)**.** *Let $n_1, n_2, \ldots, n_r$ be positive integers such that $\gcd(n_i, n_j) = 1$ for $i \neq j$. Then the system of linear congruences*

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x &\equiv a_r \pmod{n_r} \end{aligned}$$

has a simultaneous solution, which is unique modulo the integer $n_1 n_2 \cdots n_r$.

Proof. We start by forming the product $n = n_1 n_2 \cdots n_r$. For each $k = 1, 2, \ldots, r$, let

$$N_k = \frac{n}{n_k} = n_1 \cdots n_{k-1} n_{k+1} \cdots n_r.$$

In words, N_k is the product of all the integers n_i with the factor n_k omitted. By hypothesis, the n_i are relatively prime in pairs, so that $\gcd(N_k, n_k) = 1$. According to the theory of a single linear congruence, it is therefore possible to solve the congruence $N_k x \equiv 1 \pmod{n_k}$; call the unique solution x_k. Our aim is to prove that the integer

$$\bar{x} = a_1 N_1 x_1 + a_2 N_2 x_2 + \cdots + a_r N_r x_r$$

is a simultaneous solution of the given system.

First, observe that $N_i \equiv 0 \pmod{n_k}$ for $i \neq k$, because $n_k \mid N_i$ in this case. The result is

$$\bar{x} = a_1 N_1 x_1 + \cdots + a_r N_r x_r \equiv a_k N_k x_k \pmod{n_k}.$$

But the integer x_k was chosen to satisfy the congruence $N_k x \equiv 1 \pmod{n_k}$, which forces

$$\bar{x} \equiv a_k \cdot 1 \equiv a_k \pmod{n_k}.$$

This shows that a solution to given system of congruences exists.

As for the uniqueness of the solution, suppose that x' is any other integer that satisfies these congruences. Then

$$\bar{x} \equiv a_k \equiv x' \pmod{n_k} \qquad k = 1, 2, \ldots, r$$

and so $n_k \mid \bar{x} - x'$ for each value of k. Because $\gcd(n_i, n_j) = 1$, Corollary 2.3.3 supplies us with the crucial point that $n_1 n_2 \cdots n_r \mid \bar{x} - x'$; hence $\bar{x} \equiv x' \pmod{n}$. □

Example 3. Solve the system

$$x \equiv 2 \pmod{3}$$
$$x \equiv 3 \pmod{5}$$
$$x \equiv 2 \pmod{7}.$$

Example 4. Solve the linear congruence

$$17x \equiv 9 \pmod{276}.$$

Theorem 4.4.3. *The system of linear congruences*

$$ax + by \equiv r \pmod{n}$$
$$cx + dy \equiv s \pmod{n}$$

has a unique solution modulo n whenever $\gcd(ad - bc, n) = 1$.

Proof. Let us multiply the first congruence of the system by d, the second congruence by b, and subtract the lower result from the upper. These calculations yield

$$(ad - bc)x \equiv dr - bs \pmod{n}. \tag{1}$$

The assumption $\gcd(ad - bc, n) = 1$ ensures that the congruence

$$(ad - bc)z \equiv 1 \pmod{n}$$

possesses a unique solution; denote the solution by t. When congruence (1) is multiplied by t, we obtain

$$x \equiv t(dr - bs) \pmod{n}.$$

A value for y is found by a similar elimination process. That is, multiply the first congruence of the system by c, the second one by a, and subtract to end up with

$$(ad - bc)y \equiv as - cr \pmod{n}. \tag{2}$$

Multiplication of this congruence by t leads to

$$y \equiv t(as - cr) \pmod{n}.$$ □

Example 5. Solve the system

$$7x + 3y \equiv 10 \pmod{16}$$
$$2x + 5y \equiv 9 \pmod{16}.$$

Chapter 5

Fermat's Theorem

5.2 Fermat's Little Theorem and Pseudoprimes

Theorem 5.2.1 (Fermat's Theorem)**.** *Let p be a prime and suppose that $p \nmid a$. Then $a^{p-1} \equiv 1 \pmod{p}$.*

Proof. We begin by considering the first $p-1$ positive multiples of a; that is, the integers

$$a, 2a, 3a, \ldots, (p-1)a.$$

None of these numbers is congruent modulo p to any other, nor is any congruent to zero. Indeed, if it happened that

$$ra \equiv sa \pmod{p} \qquad 1 \leq r < s \leq p-1,$$

then a could be canceled to give $r \equiv s \pmod{p}$, which is impossible. Therefore, the previous set of integers must be congruent modulo p to $1, 2, 3, \ldots, p-1$, taken in some order. Multiplying all these congruences together, we find that

$$a \cdot 2a \cdot 3a \cdots (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \pmod{p},$$

whence

$$a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}.$$

Once $(p-1)!$ is canceled from both sides of the preceding congruence (this is possible because since $p \nmid (p-1)!$), our line of reasoning culminates in the statement that $a^{p-1} \equiv 1 \pmod{p}$, which is Fermat's theorem. □

Corollary 5.2.1. *If p is a prime, then $a^p \equiv a \pmod{p}$ for any integer a.*

Proof. When $p \mid a$, the statement obviously holds; for, in this setting, $a^p \equiv 0 \equiv a \pmod{p}$. If $p \nmid a$, then according to Fermat's theorem, we have $a^{p-1} \equiv 1 \pmod{p}$. When this congruence is multiplied by a, the conclusion $a^p \equiv a \pmod{p}$ follows. □

Example 1. Use Fermat's theorem to show that 117 is composite.

Example 2. If p and q are distinct primes, prove that

$$p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}.$$

***Lemma* 5.2.1:** If p and q are distinct primes with $a^p \equiv a \pmod{q}$ and $a^q \equiv a \pmod{p}$, then $a^{pq} \equiv a \pmod{pq}$.

Proof. The last corollary tells us that $(a^q)^p = a^q \pmod{p}$, whereas $a^q \equiv a \pmod{p}$ holds by hypothesis. Combining these congruences, we obtain $a^{pq} \equiv a \pmod{p}$ or, in different terms, $p \mid a^{pq} - a$. In an entirely similar manner, $q \mid a^{pq} - a$. Corollary 2.3.3 now yields $pq \mid a^{pq} - a$, which can be recast as $a^{pq} \equiv a \mod pq$. □

Example 3. Show that $2^{340} \equiv 1 \pmod{341}$ to illustrate that the converse to Fermat's theorem is false.

Definition 5.2.1. A composite integer n is called pseudoprime whenever $n \mid 2^n - 2$.

Theorem 5.2.2. *If n is an odd pseudoprime, then $M_n = 2^n - 1$ is a larger one.*

Proof. Because n is a composite number, we can write $n = rs$, with $1 < r \leq s < n$. Then, according to Example 6 of Section 2.3, $2^r - 1 \mid 2^n - 1$, or equivalently $2^r - 1 \mid M_n$, making M_n composite. By our hypotheses, $2^n \equiv 2 \pmod{n}$; hence $2^n - 2 = kn$ for some integer k. It follows that

$$2^{M_n - 1} = 2^{2^n - 2} = 2^{kn}.$$

This yields

$$\begin{aligned} 2^{M_n - 1} - 1 &= 2^{kn} - 1 \\ &= (2^n - 1)(2^{n(k-1)} + 2^{n(k-2)} + \cdots + 2^n + 1) \\ &= M_n(2^{n(k-1)} + 2^{n(k-2)} + \cdots + 2^n + 1) \\ &\equiv 0 \pmod{M_n}. \end{aligned}$$

We see immediately that $2^{M_n} - 2 \equiv 0 \pmod{M_n}$, in light of which M_n is a pseudoprime. □

Definition 5.2.2. A composite integer n that is a pseudoprime to every base a, that is, $a^{n-1} \equiv 1 \pmod{n}$ for all integers a with $\gcd(a, n) = 1$, is called an absolute pseudoprime or Carmichael number.

Theorem 5.2.3. *Let n be a composite square-free integer, say, $n = p_1 p_2 \cdots p_r$, where the p_i are distinct primes. If $p_i - 1 \mid n - 1$ for $i = 1, 2, \ldots, r$, then n is an absolute pseudoprime.*

Proof. Suppose that a is an integer satisfying $\gcd(a, n) = 1$, so that $\gcd(a, p_i) = 1$ for each i. Then Fermat's theorem yields $p_i \mid a^{p_i - 1} - 1$. From the divisibility hypothesis $p_i - 1 \mid n - 1$, we have $p_i \mid a^{n-1} - 1$, and therefore $p_i \mid a^n - a$ for all a and $i = 1, 2, \ldots, r$. As a result of Corollary 2.3.3, we end up with $n \mid a^n - a$ which makes n an absolute pseudoprime. □

Example 4. Prove that any integer of the form

$$n = (6k + 1)(12k + 1)(18k + 1)$$

is an absolute pseudoprime if all three factors are prime; hence $1729 = 7 \cdot 13 \cdot 19$ is an absolute pseudoprime.

5.3 Wilson's Theorem

Theorem 5.3.1 (Wilson)**.** *If p is a prime, then* $(p-1)! \equiv -1 \pmod{p}$.

Proof. Dismissing the cases $p = 2$ and $p = 3$ as being evident, let us take $p > 3$. Suppose that a is any one of the $p-1$ positive integers

$$1, 2, 3, \ldots, p-1$$

and consider the linear congruence $ax \equiv 1 \pmod{p}$. Then $\gcd(a, p) = 1$. By Theorem 4.4.1, this congruence admits a unique solution modulo p; hence, there is a unique integer a', with $1 \leq a' \leq p-1$, satisfying $aa' \equiv 1 \pmod{p}$.

Because p is prime, $a = a'$ if and only if $a = 1$ or $a = p-1$. Indeed, the congruence $a^2 \equiv 1 \pmod{p}$ is equivalent to $(a-1) \cdot (a+1) \equiv 0 \pmod{p}$. Therefore, either $a - 1 \equiv 0 \pmod{p}$, in which case $a = 1$, or $a + 1 \equiv 0 \pmod{p}$, in which case $a = p-1$.

If we omit the number 1 and $p-1$, the effect is to group the remaining integers $2, 3, \ldots, p-2$ into pairs a, a', where $a \neq a'$, such that their product $aa' \equiv 1 \pmod{p}$. When these $(p-2)/2$ congruences are multiplied together and the factors rearranged, we get

$$2 \cdot 3 \cdots (p-2) \equiv 1 \pmod{p}$$

or rather

$$(p-2)! \equiv 1 \pmod{p}.$$

Now multiply by $p-1$ to obtain the congruence

$$(p-1)! \equiv p - 1 \equiv -1 \pmod{p},$$

as was to be proved. □

Example 1. Illustrate Wilson's theorem with $p = 13$.

Example 2. Given a prime number p, establish the congruence

$$(p-1)! \equiv p-1 \pmod{1+2+3+\cdots+(p-1)}.$$

Theorem 5.3.2. *The quadratic congruence $x^2+1 \equiv 0 \pmod{p}$, where p is an odd prime, has a solution if and only if $p \equiv 1 \pmod{4}$.*

Proof. Let a be any solution of $x^2+1 \equiv 0 \pmod{p}$, so that $a^2 \equiv -1 \pmod{p}$. Because $p \nmid a$, the outcome of applying Fermat's theorem is

$$1 \equiv a^{p-1} \equiv (a^2)^{(p-1)/2} \equiv (-1)^{(p-1)/2} \pmod{p}.$$

The possibility that $p = 4k+3$ for some k does not arise. If it did, we would have

$$(-1)^{(p-1)/2} = (-1)^{2k+1} = -1,$$

hence, $1 \equiv -1 \pmod{p}$. The net result of this is that $p \mid 2$, which is patently false. Therefore, p must be of the form $4k+1$.

Now for the opposite direction. In the product

$$(p-1)! = 1 \cdot 2 \cdots \frac{p-1}{2} \cdot \frac{p+1}{2} \cdots (p-2)(p-1)$$

we have the congruences

$$\begin{aligned} p-1 &\equiv -1 \pmod{p} \\ p-2 &\equiv -2 \pmod{p} \\ &\vdots \\ \frac{p+1}{2} &\equiv -\frac{p-1}{2} \pmod{p}. \end{aligned}$$

Rearranging the factors produces

$$\begin{aligned}(p-1)! &\equiv 1 \cdot (-1) \cdot 2 \cdot (-2) \cdots \frac{p-1}{2} \cdot \left(-\frac{p-1}{2}\right) \pmod{p} \\ &\equiv (-1)^{(p-1)/2} \left(1 \cdot 2 \cdots \frac{p-1}{2}\right)^2 \pmod{p}\end{aligned}$$

because there are $(p-1)/2$ minus signs involved. It is at this point that Wilson's theorem can be brought to bear; for, $(p-1)! \equiv -1 \pmod{p}$, whence

$$-1 \equiv (-1)^{(p-1)/2} \left[\left(\frac{p-1}{2}\right)!\right]^2 \pmod{p}.$$

The conclusion is that the integer $[(p-1)/2]!$ satisfies the quadratic congruence $x^2 + 1 \equiv 0 \pmod{p}$. □

Example 3. Show that if $p = 4k + 3$ is prime and $a^2 + b^2 \equiv 0 \pmod{p}$, then $a \equiv b \equiv 0 \pmod{p}$.

5.4 The Fermat-Kraitchik Factorization Method

Example 1. Factor the integer $n = 119143$.

Example 2. Factor the integer $n = 2189$.

Example 3. Factor the integer $n = 12499$.

Chapter 6

Number-Theoretic Functions

6.1 The Sum and Number of Divisors

Definition 6.1.1. Given a positive integer n, let $\tau(n)$ denote the number of positive divisors of n and $\sigma(n)$ denote the sum of these divisors.

Theorem 6.1.1. *If $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ is the prime factorization of $n > 1$, then the positive divisors of n are precisely those integers d of the form*

$$d = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$$

where $0 \leq a_i \leq k_i$ $(i = 1, 2, \ldots, r)$.

Proof. Note that the divisor $d = 1$ is obtained when $a_1 = a_2 = \cdots = a_r = 0$, and n itself occurs when $a_1 = k_1, a_2 = k_2, \ldots, a_r = k_r$. Suppose that d divides n nontrivially; say, $n = dd'$, where $d > 1$, $d' > 1$. Express both d and d' as products of (not necessarily distinct) primes:

$$d = q_1 q_2 \cdots q_s \qquad d' = t_1 t_2 \cdots t_u$$

with q_i, t_j prime. Then

$$p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r} = q_1 \cdots q_s t_1 \cdots t_u$$

are two prime factorizations of the positive integer n. By the uniqueness of the prime factorization, each prime q_i must be one of the p_j. Collecting the equal primes into a single integral power, we get

$$d = q_1 q_2 \cdots q_s = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$$

where the possibility that $a_i = 0$ is allowed.

Conversely, every number $d = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$ $(0 \leq a_i \leq k_i)$ turns out to be a divisor of n. For we can write

$$\begin{aligned} n &= p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r} \\ &= (p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r})(p_1^{k_1 - a_1} p_2^{k_2 - a_2} \cdots p_r^{k_r - a_r}) \\ &= dd' \end{aligned}$$

with $d' = p_1^{k_1 - a_1} p_2^{k_2 - a_2} \cdots p_r^{k_r - a_r}$ and $k_i - a_i \geq 0$ for each i. Then $d' > 0$ and $d \mid n$. □

Theorem 6.1.2. *If $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ is the prime factorization of $n > 1$, then*

(a) $\tau(n) = (k_1 + 1)(k_2 + 1) \cdots (k_r + 1)$, *and*

(b) $\sigma(n) = \dfrac{p_1^{k_1+1} - 1}{p_1 - 1} \dfrac{p_2^{k_2+1} - 1}{p_2 - 1} \cdots \dfrac{p_r^{k_r+1} - 1}{p_r - 1}$.

Proof. According to Theorem 6.1.1, the positive divisors of n are precisely those integers

$$p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$$

where $0 \leq a_i \leq k_i$. There are $k_1 + 1$ choices for the exponent a_1; $k_2 + 1$ choices for $a_2, \ldots$; and $k_r + 1$ choices for a_r. Hence, there are

$$(k_1 + 1)(k_2 + 1) \cdots (k_r + 1)$$

possible divisors of n.

To evaluate $\sigma(n)$, consider the product

$$\begin{aligned} (1 + p_1 + p_1^2 + \cdots + p_1^{k_1})(1 + p_2 + p_2^2 + \cdots + p_2^{k_2}) \\ \cdots (1 + p_r + p_r^2 + \cdots + p_r^{k_r}). \end{aligned}$$

Each positive divisor of n appears once and only once as a term in the expansion of this product, so that

$$\sigma(n) = (1 + p_1 + p_1^2 + \cdots p_1^{k_1}) \cdots (1 + p_r + p_r^2 + \cdots + p_r^{k_r}).$$

Applying the formula for the sum of a finite geometric series to the ith factor on the right-hand side, we get

$$1 + p_i + p_i^2 + \cdots + p_i^{k_i} = \frac{p_i^{k_i+1} - 1}{p_i - 1}.$$

It follows that

$$\sigma(n) = \frac{p_1^{k_1+1} - 1}{p_1 - 1} \frac{p_2^{k_2+1} - 1}{p_2 - 1} \cdots \frac{p_r^{k_r+1} - 1}{p_r - 1}.$$

□

Example 1. Find τ and σ for the number 180.

Example 2. If n is a square-free integer, prove that $\tau(n) = 2^r$, where r is the number of prime divisors of n.

Definition 6.1.2. A number-theoretic function f is said to be multiplicative if

$$f(mn) = f(m)f(n)$$

whenever $\gcd(m, n) = 1$.

Theorem 6.1.3. *The functions τ and σ are both multiplicative functions.*

Proof. Let m and n be relatively prime integers. Because the result is trivially true if either m or n is equal to 1, we may assume that $m > 1$ and $n > 1$. If

$$m = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r} \qquad \text{and} \qquad n = q_1^{j_1} q_2^{j_2} \cdots q_s^{j_s}$$

are the prime factorizations of m and n, then because $\gcd(m, n) = 1$, no p_i can occur among the q_j. It follows that the prime factorization of the product mn is given by

$$mn = p_1^{k_1} \cdots p_r^{k_r} q_1^{j_1} \cdots q_s^{j_s}.$$

Appealing to Theorem 6.1.2, we obtain

$$\begin{aligned} \tau(mn) &= [(k_1 + 1) \cdots (k_r + 1)][(j_1 + 1) \cdots (j_s + 1)] \\ &= \tau(m)\tau(n). \end{aligned}$$

In a similar fashion, Theorem 6.1.2 gives

$$\begin{aligned} \sigma(mn) &= \left[\frac{p_1^{k_1+1} - 1}{p_1 - 1} \cdots \frac{p_r^{k_r+1} - 1}{p_r - 1} \right] \left[\frac{q_1^{j_1+1} - 1}{q_1 - 1} \cdots \frac{q_s^{j_s+1} - 1}{q_s - 1} \right] \\ &= \sigma(m)\sigma(n). \end{aligned}$$

Thus, τ and σ are multiplicative functions. □

***Lemma* 6.1.1:** If $\gcd(m,n) = 1$, then the set of positive divisors of mn consists of all products $d_1 d_2$, where $d_1 \mid m$, $d_2 \mid n$, and $\gcd(d_1, d_2) = 1$; furthermore, these products are all distinct.

Proof. It is harmless to assume that $m > 1$ and $n > 1$; let $m = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ and $n = q_1^{j_1} q_2^{j_2} \cdots q_s^{j_s}$ be their respective prime factorizations. Inasmuch as the primes $p_1, \ldots, p_r, q_1, \ldots, q_s$ are all distinct, the prime factorization of mn is

$$mn = p_1^{k_1} \cdots p_r^{k_r} q_1^{j_1} \cdots q_s^{j_s}.$$

Hence, any positive divisor d of mn will be uniquely representable in the form

$$d = p_1^{a_1} \cdots p_r^{a_r} q_1^{b_1} \cdots q_s^{b_s} \qquad 0 \le a_i \le k_i, 0 \le b_i \le j_i.$$

This allows us to write d as $d = d_1 d_2$, where $d_1 = p_1^{a_1} \cdots p_r^{a_r}$ divides m and $d_2 = q_1^{b_1} \cdots q_s^{b_s}$ divides n. Because no p_i is equal to any q_j, we surely must have $\gcd(d_1, d_2) = 1$. □

Theorem 6.1.4. *If f is a multiplicative function and F is defined by*

$$F(n) = \sum_{d \mid n} f(d)$$

then F is also multiplicative.

Proof. Let m and n be relatively prime integers. Then

$$\begin{aligned} F(mn) &= \sum_{d \mid mn} f(d) \\ &= \sum_{\substack{d_1 \mid m \\ d_2 \mid n}} f(d_1 d_2) \end{aligned}$$

because every divisor d of mn can be uniquely written as a product of a divisor d_1 of m and a divisor d_2 of n, where $\gcd(d_1, d_2) = 1$. By the definition of a multiplicative function,

$$f(d_1 d_2) = f(d_1) f(d_2).$$

It follows that

$$\begin{aligned} F(mn) &= \sum_{\substack{d_1 \mid m \\ d_2 \mid n}} f(d_1 d_2) \\ &= \left(\sum_{d_1 \mid m} f(d_1) \right) \left(\sum_{d_2 \mid n} f(d_2) \right) \\ &= F(m) F(n). \end{aligned}$$

□

Example 3. Illustrate Theorem 6.1.4 using $n = 24$.

Corollary 6.1.1. *The functions τ and σ are multiplicative functions.*

Proof. The constant function $f(n) = 1$ is multiplicative, as is the identity function $f(n) = n$. Because τ and σ may be represented in the form

$$\tau(n) = \sum_{d|n} 1 \qquad \text{and} \qquad \sigma(n) = \sum_{d|n} d$$

the stated result follows immediately from Theorem 6.1.4. □

Example 4. Let $\omega(n)$ denoted the number of distinct prime divisors of $n > 1$, with $\omega(1) = 0$. For instance, $\omega(360) = \omega(2^3 \cdot 3^2 \cdot 5) = 3$.

(a) Show that $2^{\omega(n)}$ is a multiplicative function.

(b) For a positive integer n, establish the formula

$$\tau(n^2) = \sum_{d|n} 2^{\omega(d)}.$$

6.2 The Möbius Inversion Formula

Definition 6.2.1. For a positive integer n, define μ by the rules

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } p^2 \mid n \text{ for some prime } p \\ (-1)^r & \text{if } n = p_1 p_2 \cdots p_r, \text{ where } p_i \text{ are distinct primes.} \end{cases}$$

Theorem 6.2.1. *The function μ is a multiplicative function.*

Proof. We want to show that $\mu(mn) = \mu(m)\mu(n)$, whenever m and n are relatively prime. If either $p^2 \mid m$ or $p^2 \mid n$, p a prime, then $p^2 \mid mn$; hence, $\mu(mn) = 0 = \mu(m)\mu(n)$, and the formula holds trivially. We therefore may assume that both m and n are square-free integers. Say, $m = p_1 p_2 \cdots p_r$, $n = q_1 q_2 \cdots q_s$, with all the primes p_i and q_j being distinct. Then

$$\begin{aligned} \mu(mn) &= \mu(p_1 \cdots p_r q_1 \cdots q_s) = (-1)^{r+s} \\ &= (-1)^r (-1)^s = \mu(m)\mu(n), \end{aligned}$$

which completes the proof. □

Theorem 6.2.2. *For each positive integer $n \geq 1$,*

$$\sum_{d \mid n} \mu(d) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n > 1 \end{cases}$$

where d runs through the positive divisors of n.

Proof. Suppose $n > 1$ and put

$$F(n) = \sum_{d \mid n} \mu(d).$$

We first calculate $F(n)$ for the power of a prime, say, $n = p^k$. The positive divisors of p^k are just the $k+1$ integers $1, p, p^2, \ldots, p^k$, so that

$$\begin{aligned} F(p^k) = \sum_{d \mid p^k} \mu(d) &= \mu(1) + \mu(p) + \mu(p^2) + \cdots + \mu(p^k) \\ &= \mu(1) + \mu(p) = 1 + (-1) = 0. \end{aligned}$$

Because μ is multiplicative, Theorem 6.1.4 guarantees that F also is multiplicative. Thus, if the canonical factorization of n is $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$, then $F(n)$ is the product of the values assigned to F for the prime powers in this representation:

$$F(n) = F\left(p_1^{k_1}\right) F\left(p_2^{k_2}\right) \cdots F\left(p_r^{k_r}\right) = 0.$$ □

Example 1. The Mangoldt function Λ is defined by

$$\Lambda(n) = \begin{cases} \log p & \text{if } n = p^k, \text{ where } p \text{ is a prime and } k \geq 1 \\ 0 & \text{otherwise.} \end{cases}$$

Prove that $\Lambda(n) = \sum_{d|n} \mu(n/d) \log d = -\sum_{d|n} \mu(d) \log d$.

Theorem 6.2.3 (The Möbius Inversion Formula)**.** *Let F and f be two number-theoretic functions related by the formula*

$$F(n) = \sum_{d|n} f(d).$$

Then

$$f(n) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right) = \sum_{d|n} \mu\left(\frac{n}{d}\right) F(d).$$

Proof. The two sums mentioned in the conclusion of the theorem are seen to be the same upon replacing the dummy index d by $d' = n/d$; as d ranges over all positive divisors of n, so does d'.

Carrying out the required computation, we get

$$\begin{aligned} \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right) &= \sum_{d|n} \left(\mu(d) \sum_{c|(n/d)} f(c) \right) \\ &= \sum_{d|n} \left(\sum_{c|(n/d)} \mu(d) f(c) \right). \end{aligned} \tag{1}$$

It is easily verified that $d \mid n$ and $c \mid (n/d)$ if and only if $c \mid n$ and $d \mid (n/c)$. Because of this, the last expression in equation (1) becomes

$$\begin{aligned} \sum_{d|n} \left(\sum_{c|(n/d)} \mu(d) f(c) \right) &= \sum_{c|n} \left(\sum_{d|(n/c)} f(c) \mu(d) \right) \\ &= \sum_{c|n} \left(f(c) \sum_{d|(n/c)} \mu(d) \right). \end{aligned} \tag{2}$$

In compliance with Theorem 6.2.2, the sum $\sum_{d|(n/c)} \mu(d)$ must vanish except when $n/c = 1$ (that is, when $n = c$), in which case it is equal to 1; the upshot is that the right-hand side of equation (2) simplifies to

$$\begin{aligned} \sum_{c|n} \left(f(c) \sum_{d|(n/c)} \mu(d) \right) &= \sum_{c=n} f(c) \cdot 1 \\ &= f(n), \end{aligned}$$

giving us the stated result. □

Theorem 6.2.4. *If F is a multiplicative function*

$$F(n) = \sum_{d|n} f(d)$$

then f is also multiplicative.

Proof. Let m and n be relatively prime positive integers. We recall that any divisor d of mn can be uniquely written as $d = d_1 d_2$, where $d_1 \mid m$, $d_2 \mid n$, and $\gcd(d_1, d_2) = 1$. Thus, using the inversion formula,

$$\begin{aligned} f(mn) &= \sum_{d \mid mn} \mu(d) F\left(\frac{mn}{d}\right) \\ &= \sum_{\substack{d_1 \mid m \\ d_2 \mid n}} \mu(d_1 d_2) F\left(\frac{mn}{d_1 d_2}\right) \\ &= \sum_{\substack{d_1 \mid m \\ d_2 \mid n}} \mu(d_1)\mu(d_2) F\left(\frac{m}{d_1}\right) F\left(\frac{n}{d_2}\right) \\ &= \sum_{d_1 \mid m} \mu(d_1) F\left(\frac{m}{d_1}\right) \sum_{d_2 \mid n} \mu(d_2) F\left(\frac{n}{d_2}\right) \\ &= f(m) f(n), \end{aligned}$$

which is the assertion of the theorem. Needless to say, the multiplicative character of μ and of F is crucial to the previous calculation. □

Example 2. Let $S(n)$ denote the number of square-free divisors of n. Establish that

$$S(n) = \sum_{d \mid n} |\mu(d)| = 2^{\omega(n)}$$

where $\omega(n)$ is the number of distinct prime divisors of n.

6.3 The Greatest Integer Function

Definition 6.3.1. For an arbitrary real number x, we denote by $[x]$ the largest integer less than or equal to x; that is, $[x]$ is the unique integer satisfying $x - 1 < [x] \leq x$.

Theorem 6.3.1. *If n is a positive integer and p a prime, then the exponent of the highest power of p that divides $n!$ is*

$$\sum_{k=1}^{\infty} \left[\frac{n}{p^k} \right],$$

where the series is finite, because $[n/p^k] = 0$ for $p^k > n$.

Proof. Among the first n positive integers, those divisible by p are $p, 2p, \ldots, tp$, where t is the largest integer such that $tp \leq n$; in other words, t is the largest integer less than or equal to n/p (which is to say $t = [n/p]$). Thus, there are exactly $[n/p]$ multiples of p occurring in the product that defines $n!$, namely,

$$p, 2p, \ldots, \left[\frac{n}{p} \right] p. \tag{1}$$

The exponent of p in the prime factorization of $n!$ is obtained by adding to the number of integers in equation (1), the number of integers among $1, 2, \ldots, n$ divisible by p^2, and then the number divisible by p^3, and so on. Reasoning as in the first paragraph, the integers between 1 and n that are divisible by p^2 are

$$p^2, 2p^2, \ldots, \left[\frac{n}{p^2} \right] p^2, \tag{2}$$

which are $[n/p^2]$ in number. Of these, $[n/p^3]$ are again divisible by p:

$$p^3, 2p^3, \ldots, \left[\frac{n}{p^3} \right] p^3. \tag{3}$$

After a finite number of repetitions of this process, we are led to conclude that the total number of times p divides $n!$ is

$$\sum_{k=1}^{\infty} \left[\frac{n}{p^k} \right]. \qquad \square$$

Example 1. Find the number of zeros with which the decimal representation of 50! terminates.

Example 2. For an integer $n \geq 0$, show that $[n/2] - [-n/2] = n$.

Theorem 6.3.2. *If n and r are positive integers with $1 \leq r < n$, then the binomial coefficient*

$$\binom{n}{r} = \frac{n!}{r!(n-r)!}$$

is also an integer.

Proof. The argument rests on the observation that if a and b are arbitrary real numbers, then $[a+b] \geq [a] + [b]$. In particular, for each prime factor p of $r!(n-r)!$,

$$\left[\frac{n}{p^k}\right] \geq \left[\frac{r}{p^k}\right] + \left[\frac{(n-r)}{p^k}\right] \qquad k = 1, 2, \ldots.$$

Adding these inequalities, we obtain

$$\sum_{k\geq 1} \left[\frac{n}{p^k}\right] \geq \sum_{k\geq 1} \left[\frac{r}{p^k}\right] + \sum_{k\geq 1} \left[\frac{(n-r)}{p^k}\right]. \tag{4}$$

The left-hand side of equation (4) gives the exponent of the highest power of the prime p that divides $n!$, whereas the right-hand side equals the highest power of this prime contained $r!(n-r)!$. Hence, p appears in the numerator of $n!/r!(n-r)!$ at least as many times as it occurs in the denominator. Because this holds true for every prime divisor of the denominator, $r!(n-r)!$ must divide $n!$, making $n!/r!(n-r)!$ an integer. □

Corollary 6.3.1. *For a positive integer r, the product of any r consecutive positive integers is divisible by $r!$.*

Proof. The product of r consecutive positive integers, the largest of which is n, is

$$n(n-1)(n-2)\cdots(n-r+1).$$

Now we have

$$n(n-1)\cdots(n-r+1) = \left(\frac{n!}{r!(n-r)!}\right) r!.$$

Because $n!/r!(n-r)!$ is an integer by the theorem, it follows that $r!$ must divide the product $n(n-1)\cdots(n-r+1)$, as asserted. □

Theorem 6.3.3. *Let f and F be number-theoretic functions such that*

$$F(n) = \sum_{d|n} f(d).$$

Then, for any positive integer N,

$$\sum_{n=1}^{N} F(n) = \sum_{k=1}^{N} f(k) \left[\frac{N}{k}\right].$$

Proof. We begin by noting that

$$\sum_{n=1}^{N} F(n) = \sum_{n=1}^{N} \sum_{d|n} f(d). \tag{5}$$

The strategy is to collect terms with equal values of $f(d)$ in this double sum. For a fixed positive integer $k \leq N$, the term $f(k)$ appears in $\sum_{d|n} f(d)$ if and only if k is a divisor of n. (Because each integer has itself as a divisor, the right-hand side of equation (5) includes $f(k)$, at least once.) Now, to calculate the number of sums $\sum_{d|n} f(d)$ in which $f(k)$ occurs as a term, it is sufficient to find the number of integers among $1, 2, \ldots, N$, which are divisible by k. There are exactly $[N/k]$ of them:

$$k, 2k, 3k, \ldots, \left[\frac{N}{k}\right] k.$$

Thus, for each k such that $1 \leq k \leq N$, $f(k)$ is a term of the sum $\sum_{d|n} f(d)$ for $[N/k]$ different positive integers less than or equal to N. Knowing this, we may rewrite the double sum in equation (5) as

$$\sum_{n=1}^{N} \sum_{d|n} f(d) = \sum_{k=1}^{N} f(k) \left[\frac{N}{k}\right]$$

and our task is complete. □

Corollary 6.3.2. *If N is a positive integer, then*

$$\sum_{n=1}^{N} \tau(n) = \sum_{n=1}^{N} \left[\frac{N}{n}\right].$$

Proof. Noting that $\tau(n) = \sum_{d|n} 1$, we may write τ for F and take f to be the constant function $f(n) = 1$ for all n. □

Corollary 6.3.3. *If N is a positive integer, then*

$$\sum_{n=1}^{N} \sigma(n) = \sum_{n=1}^{N} n \left[\frac{N}{n}\right].$$

Example 3. Apply the preceding corollaries to in the case $N = 6$.

Example 4. Given a positive integer N, show the following:

(a) $\sum_{n=1}^{N} \mu(n)[N/n] = 1$.

(b) $|\sum_{n=1}^{N} \mu(n)/n| \leq 1$.

6.4 An Application to the Calendar

Theorem 6.4.1. *The date with month m, day d, year $Y = 100c + y$ where $c \geq 16$ and $0 \leq y < 100$, has weekday number*

$$w \equiv d + [(2.6)m - 0.2] - 2c + y + \left[\frac{c}{4}\right] + \left[\frac{y}{4}\right] \pmod 7$$

provided that March is taken as the first month of the year and January and February are assumed to be the eleventh and twelfth months of the previous year.

Proof. The weekday number D_Y for March 1 of any year $Y > 1600$ will satisfy the congruence

$$D_Y \equiv D_{1600} + (Y - 1600) + L \pmod 7, \tag{1}$$

where L is the number of leap year days between March 1, 1600, and March 1 of the year Y.

To find L, observe that since $[x - a] = [x] - a$ whenever a is an integer, the number of years n in the interval $1600 < n \leq Y$ that are divisible by 4 is given by

$$\left[\frac{Y - 1600}{4}\right] = \left[\frac{Y}{4} - 400\right] = \left[\frac{Y}{4}\right] - 400.$$

Likewise, the number of elapsed century years is

$$\left[\frac{Y - 1600}{100}\right] = \left[\frac{Y}{100} - 16\right] = \left[\frac{Y}{100}\right] - 16,$$

whereas among those there are

$$\left[\frac{Y - 1600}{400}\right] = \left[\frac{Y}{400} - 4\right] = \left[\frac{Y}{400}\right] - 4$$

century years that are divisible by 400. Taken together, these statements yield

$$\begin{aligned} L &= \left(\left[\frac{Y}{4}\right] - 400\right) - \left(\left[\frac{Y}{100}\right] - 16\right) + \left(\left[\frac{Y}{400}\right] - 4\right) \\ &= \left[\frac{Y}{4}\right] - \left[\frac{Y}{100}\right] + \left[\frac{Y}{400}\right] - 388. \end{aligned}$$

By writing the year Y as $Y = 100c + y$, the previous expression for L becomes

$$\begin{aligned} L &= \left[25c + \frac{y}{4}\right] - \left[c + \frac{y}{100}\right] + \left[\frac{c}{4} + \frac{y}{400}\right] - 388 \\ &= 24c + \left[\frac{y}{4}\right] + \left[\frac{c}{4}\right] - 388. \end{aligned}$$

Then the congruence for D_Y appears as

$$D_Y \equiv 3 + (100c + y - 1600) + 24c + \left[\frac{y}{4}\right] + \left[\frac{c}{4}\right] - 388 \pmod 7,$$

which reduces to

$$D_Y \equiv 3 - 2c + y + \left[\frac{c}{4}\right] + \left[\frac{y}{4}\right] \pmod 7.$$

Now for $m = 1, 2, \ldots, 12$, the expression

$$[(2.6)m - 0.2] - 2 \pmod 7$$

produces the value that must be added to the day-number of March 1 to arrive at the number of the first day of each month in any year Y. Thus the number of the first day of the mth month of the year Y is given by

$$D_Y + [(2.6)m - 0.2] - 2 \pmod 7.$$

Finally, the number w of day d, month m, year $Y = 100c + y$ is determined from congruence

$$\begin{aligned} w &\equiv (d-1) + D_Y + [(2.6)m - 0.2] - 2 \pmod 7 \\ &\equiv d + [(2.6)m - 0.2] - 2c + y + \left[\frac{c}{4}\right] + \left[\frac{y}{4}\right] \pmod 7. \end{aligned}$$ □

Example 1. Calculate the day of the week on which March 1, 1990 fell.

Example 2. On what day of the week did January 14, 2020 occur?

Example 3. Find the years in the decade 2000 to 2009 when November 29 is on a Sunday.

Chapter 7

Euler's Generalization of Fermat's Theorem

7.2 Euler's Phi-Function

Definition 7.2.1. For $n \geq 1$, let $\phi(n)$ denote the number of positive integers not exceeding n that are relatively prime to n.

Theorem 7.2.1. *If p is a prime and $k > 0$, then*

$$\phi(p^k) = p^k - p^{k-1} = p^k\left(1 - \frac{1}{p}\right).$$

Proof. Clearly, $\gcd(n, p^k) = 1$ if and only if $p \nmid n$. There are p^{k-1} integers between 1 and p^k divisible by p, namely,

$$p, 2p, 3p, \ldots, (p^{k-1})p.$$

Thus, the set $\{1, 2, \ldots, p^k\}$ contains exactly $p^k - p^{k-1}$ integers that are relatively prime to p^k, and so by the definition of the phi-function, $\phi(p^k) = p^k - p^{k-1}$. □

***Lemma* 7.2.1:** Given integers a, b, c, $\gcd(a, bc) = 1$ if and only if $\gcd(a, b) = 1$ and $\gcd(a, c) = 1$.

Proof. First suppose that $\gcd(a, bc) = 1$, and put $d = \gcd(a, b)$. Then $d \mid a$ and $d \mid b$, whence $d \mid a$ and $d \mid bc$. This implies that $\gcd(a, bc) \geq d$, which forces $d = 1$. Similar reasoning gives rise to the statement $\gcd(a, c) = 1$.

For the other direction, take $\gcd(a, b) = 1 = \gcd(a, c)$ and assume that

$\gcd(a, bc) = d_1 > 1$. Then d_1 must have a prime divisor p. Because $d_1 \mid bc$, it follows that $p \mid bc$; in consequence, $p \mid b$ or $p \mid c$. If $p \mid b$, then (by virtue of the fact that $p \mid a$) we have $\gcd(a, b) \geq p$, a contradiction. In the same way, the condition $p \mid c$ leads to the equally false conclusion that $\gcd(a, c) \geq p$. Thus, $d_1 = 1$ and the lemma is proven. □

Theorem 7.2.2. *The function ϕ is a multiplicative function.*

Proof. It is required to show that $\phi(mn) = \phi(m)\phi(n)$, wherever m and n have no common factor. Because $\phi(1) = 1$, the result obviously holds if either m or n equals 1. Thus, we may assume that $m > 1$ and $n > 1$. Arrange the integers from 1 to mn in m columns of n integers each, as follows:

$$\begin{array}{ccccccc} 1 & 2 & \cdots & r & \cdots & m \\ m+1 & m+2 & & m+r & & 2m \\ 2m+1 & 2m+2 & & 2m+r & & 3m \\ \vdots & \vdots & & \vdots & & \vdots \\ (n-1)m+1 & (n-1)m+2 & & (n-1)m+r & & nm \end{array}$$

We know that $\phi(mn)$ is equal to the number of entries in this array that are relatively prime to mn; by virtue of the lemma, this is the same as the number of integers that are relatively prime to both m and n.

Now the entries in the rth column (where it is assumed that $\gcd(r, m) = 1$) are

$$r, m + r, 2m + r, \ldots, (n-1)m + r.$$

There are n integers in this sequence and no two are congruent modulo n. Indeed, if

$$km + r \equiv jm + r \pmod{n}$$

with $0 \leq k < j < n$, it would follow that $km \equiv jm \pmod{n}$. Because $\gcd(m, n) = 1$, we could cancel m from both sides of this congruence to arrive at the contradiction that $k \equiv j \pmod{n}$. Thus, the numbers in the rth column are congruent modulo n to $0, 1, 2, \ldots, n-1$, in some order. But if $s \equiv t \pmod{n}$, then $\gcd(s, n) = 1$ if and only if $\gcd(t, n) = 1$. The implication is that the rth column contains as many integers that are relatively prime to n as does the set $\{0, 1, 2, \ldots, n-1\}$, namely, $\phi(n)$ integers. Therefore, the total number of entries in the array that are relatively prime to both m and n is $\phi(m)\phi(n)$. □

Theorem 7.2.3. *If the integer $n > 1$ has the prime factorization $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$, then*

$$\begin{aligned}\phi(n) &= \left(p_1^{k_1} - p_1^{k_1-1}\right)\left(p_2^{k_2} - p_2^{k_2-1}\right)\cdots\left(p_r^{k_r} - p_r^{k_r-1}\right)\\ &= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_r}\right).\end{aligned}$$

Proof. We intend to use induction on r, the number of distinct prime factors of n. By Theorem 7.2.1, the result is true for $r = 1$. Suppose that it holds for $r = i$. Because

$$\gcd\left(p_1^{k_1} p_2^{k_2} \cdots p_i^{k_i}, p_{i+1}^{k_{i+1}}\right) = 1$$

the definition of multiplicative function gives

$$\begin{aligned}\phi\left(\left(p_1^{k_1}\cdots p_i^{k_i}\right)p_{i+1}^{k_{i+1}}\right) &= \phi\left(p_1^{k_1}\cdots p_i^{k_i}\right)\phi\left(p_{i+1}^{k_{i+1}}\right)\\ &= \phi\left(p_1^{k_1}\cdots p_i^{k_i}\right)\left(p_{i+1}^{k_{i+1}} - p_{i+1}^{k_{i+1}-1}\right).\end{aligned}$$

Invoking the induction assumption, the first factor on the right-hand side becomes

$$\phi\left(p_1^{k_1} p_2^{k_2} \cdots p_i^{k_i}\right) = \left(p_1^{k_1} - p_1^{k_1-1}\right)\left(p_2^{k_2} - p_2^{k_2-1}\right)\cdots\left(p_i^{k_i} - p_i^{k_i-1}\right)$$

and this serves to complete the induction step and with it the proof. □

Example 1. Calculate the value of $\phi(360)$.

Example 2. Prove that the equation $\phi(n) = \phi(n+2)$ is satisfied by $n = 2(2p-1)$ whenever p and $2p-1$ are both odd primes.

Theorem 7.2.4. *For $n > 2$, $\phi(n)$ is an even integer.*

Proof. First, assume that n is a power of 2, let us say that $n = 2^k$, with $k \geq 2$. By Theorem 7.2.3,

$$\phi(n) = \phi(2^k) = 2^k \left(1 - \frac{1}{2}\right) = 2^{k-1},$$

an even integer. If n does not happen to be a power of 2, then it is divisible by an odd prime p; we therefore may write n as $n = p^k m$ where $k \geq 1$ and $\gcd(p^k, m) = 1$. Exploiting the multiplicative nature of the phi-function, we obtain

$$\phi(n) = \phi(p^k)\phi(m) = p^{k-1}(p-1)\phi(m),$$

which again is even because $2 \mid p - 1$. □

Example 3. Prove that if the integer n has r distinct odd prime factors, then $2^r \mid \phi(n)$.

Example 4. If every prime that divides n also divides m, establish that $\phi(nm) = n\phi(m)$; in particular, $\phi(n^2) = n\phi(n)$ for every positive integer n.

7.3 Euler's Theorem

***Lemma* 7.3.1:** Let $n > 1$ and $\gcd(a, n) = 1$. If $a_1, a_2, \ldots, a_{\phi(n)}$ are the positive integers less than n and relatively prime to n, then

$$aa_1, aa_2, \ldots, aa_{\phi(n)}$$

are congruent modulo n to $a_1, a_2, \ldots, a_{\phi(n)}$ in some order.

Proof. Observe that no two of the integers $aa_1, aa_2, \ldots, aa_{\phi(n)}$ are congruent modulo n. For if $aa_i \equiv aa_j \pmod{n}$, with $1 \leq i < j \leq \phi(n)$, then the cancellation law yields $a_i \equiv a_j \pmod{n}$ and thus $a_i = a_j$, a contradiction. Furthermore, because $\gcd(a_i, n) = 1$ for all i and $\gcd(a, n) = 1$, Lemma 7.2.1 guarantees that each of the aa_i is relatively prime to n.

Fixing on a particular aa_i, there exists a unique integer b, where $0 \leq b < n$, for which $aa_i \equiv b \pmod{n}$. Because

$$\gcd(b, n) = \gcd(aa_i, n) = 1,$$

b must be one of the integers $a_1, a_2, \ldots, a_{\phi(n)}$. All told, this proves that the numbers $aa_1, aa_2, \ldots, aa_{\phi(n)}$ and the numbers $a_1, a_2, \ldots, a_{\phi(n)}$ are identical (modulo n) in a certain order. □

Theorem 7.3.1 (Euler)**.** *If $n \geq 1$ and $\gcd(a, n) = 1$, then $a^{\phi(n)} \equiv 1 \pmod{n}$.*

Proof. There is no harm in taking $n > 1$. Let $a_1, a_2, \ldots, a_{\phi(n)}$ be the positive integers less than n that are relatively prime to n. Because $\gcd(a, n) = 1$, it follows from the lemma that $aa_1, aa_2, \ldots, aa_{\phi(n)}$ are congruent, not necessarily in order to of appearance, to $a_1, a_2, \ldots, a_{\phi(n)}$. Then

$$\begin{aligned} aa_1 &\equiv a_1' \pmod{n} \\ aa_2 &\equiv a_2' \pmod{n} \\ \vdots &\qquad\quad \vdots \\ aa_{\phi(n)} &\equiv a_{\phi(n)}' \pmod{n} \end{aligned}$$

where $a_1', a_2', \ldots, a_{\phi(n)}'$ are the integers $a_1, a_2, \ldots, a_{\phi(n)}$ in some order. On taking the product of these $\phi(n)$ congruences, we get

$$\begin{aligned} (aa_1)(aa_2)\cdots(aa_{\phi(n)}) &\equiv a_1'a_2'\ldots a_{\phi(n)}' \pmod{n} \\ &\equiv a_1a_2\ldots a_{\phi(n)} \pmod{n} \end{aligned}$$

and so

$$a^{\phi(n)}(a_1a_2\ldots a_{\phi(n)}) \equiv a_1a_2\ldots a_{\phi(n)} \pmod{n}.$$

Because $\gcd(a_i, n) = 1$ for each i, Lemma 7.2.1 implies that $\gcd(a_1 a_2 \dots a_{\phi(n)}, n) = 1$. Therefore, we may divide both sides of the foregoing congruence by the common factor $a_1 a_2 \dots a_{\phi(n)}$, leaving us with

$$a^{\phi(n)} \equiv 1 \pmod{n}. \qquad \square$$

Corollary 7.3.1 (Fermat)**.** *If p is a prime and $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$.*

Example 1. Find the last two digits in the decimal representation of 3^{256}.

Example 2. Use Euler's Theorem to prove the Chinese Remainder Theorem.

Example 3. Show that if n is an odd integer that is not a multiple of 5, then n divides an integer all of whose digits are equal to 1.

Example 4. Use Euler's Theorem to evaluate $2^{100000} \pmod{77}$.

7.4 Some Properties of the Phi-Function

Theorem 7.4.1 (Gauss)**.** *For each positive integer $n \geq 1$,*

$$n = \sum_{d|n} \phi(d)$$

the sum being extended over all positive divisors of n.

Proof. The integers between 1 and n can be separated into classes as follows: If d is a positive divisor of n, we put the integer m in the class S_d provided that $\gcd(m, n) = d$. Stated in symbols,

$$S_d = \{m \mid \gcd(m, n) = d; 1 \leq m \leq n\}.$$

Now $\gcd(m, n) = d$ if and only if $\gcd(m/d, n/d) = 1$. Thus, the number of integers in the class S_d is equal to the number of positive integers not exceeding n/d that are relatively prime to n/d; in other words, equal to $\phi(n/d)$. Because each of the n integers in the set $\{1, 2, \ldots, n\}$ lies in exactly one class S_d, we obtain the formula

$$n = \sum_{d|n} \phi\left(\frac{n}{d}\right).$$

But as d runs through all positive divisors of n, so does n/d; hence,

$$\sum_{d|n} \phi\left(\frac{n}{d}\right) = \sum_{d|n} \phi(d),$$

which proves the theorem. □

Example 1. Illustrate the previous theorem using $n = 10$.

Theorem 7.4.2. *For $n > 1$, the sum of the positive integers less than n and relatively prime to n is $\frac{1}{2}n\phi(n)$.*

Proof. Let $a_1, a_2, \ldots, a_{\phi(n)}$ be the positive integers less than n and relatively prime to n. Now because $\gcd(a, n) = 1$ if and only if $\gcd(n - a, n) = 1$, the numbers $n-a_1$, $n-a_2, \ldots, n-a_{\phi(n)}$ are equal in some order to $a_1, a_2, \ldots, a_{\phi(n)}$. Thus,

$$\begin{aligned} a_1 + a_2 + \cdots + a_{\phi(n)} &= (n - a_1) + (n - a_2) + \cdots + (n - a_{\phi(n)}) \\ &= \phi(n)n - (a_1 + a_2 + \cdots + a_{\phi(n)}). \end{aligned}$$

Hence,

$$2(a_1 + a_2 + \cdots + a_{\phi(n)}) = \phi(n)n,$$

leading to the stated conclusion. □

Example 2. Illustrate the preceding theorem for the case where $n = 30$.

Theorem 7.4.3. *For any positive integer n,*

$$\phi(n) = n \sum_{d|n} \frac{\mu(d)}{d}.$$

Proof. If we apply the Möbius inversion formula to

$$F(n) = n = \sum_{d|n} \phi(d)$$

the result is

$$\begin{aligned} \phi(n) &= \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right) \\ &= \sum_{d|n} \mu(d) \frac{n}{d}. \end{aligned}$$

□

Example 3. For a positive integer n, prove that

$$\sum_{d|n} \mu^2(d)\phi(d) = \frac{n}{\phi(n)}.$$

Example 4. Given an integer n, prove that there exists at least one k for which $n \mid \phi(k)$.

Chapter 8

Primitive Roots and Indices

8.1 The Order of an Integer Modulo n

Definition 8.1.1. Let $n > 1$ and $\gcd(a, n) = 1$. The order of a modulo n is the smallest positive integer k such that $a^k \equiv 1 \pmod{n}$.

Theorem 8.1.1. *Let the integer a have order k modulo n. Then $a^h \equiv 1 \pmod{n}$ if and only if $k \mid h$; in particular, $k \mid \phi(n)$.*

Proof. Suppose that we begin with $k \mid h$, so that $h = jk$ for some integer j. Because $a^k \equiv 1 \pmod{n}$, Theorem 4.2.2 yields $(a^k)^j \equiv 1^j \pmod{n}$ or $a^h \equiv 1 \pmod{n}$.

Conversely, let h be any positive integer satisfying $a^h \equiv 1 \pmod{n}$. By the Division Algorithm, there exist q and r such that $h = qk + r$, where $0 \leq r < k$. Consequently,

$$a^h = a^{qk+r} = (a^k)^q a^r.$$

By hypothesis, both $a^h \equiv 1 \pmod{n}$ and $a^k \equiv 1 \pmod{n}$, the implication of which is that $a^r \equiv 1 \pmod{n}$. Because $0 \leq r < k$, we end up with $r = 0$; otherwise, the choice of k as the smallest positive integer such that $a^k \equiv 1 \pmod{n}$ is contradicted. Hence, $h = qk$, and $k \mid h$. □

Example 1. Prove that $\phi(2^n - 1)$ is a multiple of n for any $n > 1$.

Theorem 8.1.2. *If the integer a has order k modulo n, then $a^i = a^j \pmod{n}$ if and only if $i \equiv j \pmod{k}$.*

Proof. First, suppose that $a^i \equiv a^j \pmod{n}$, where $i \geq j$. Because a is relatively prime to n, we may cancel a power of a to obtain $a^{i-j} \equiv 1 \pmod{n}$. According to Theorem 8.1.1, this last congruence holds only if $k \mid i - j$, which is just another way of saying that $i \equiv j \pmod{k}$.

Conversely, let $i \equiv j \pmod{k}$. Then we have $i = j + qk$ for some integer q. By the definition of k, $a^k \equiv 1 \pmod{n}$, so that

$$a^i \equiv a^{j+qk} \equiv a^j (a^k)^q \equiv a^j \pmod{n},$$

which is the desired conclusion. □

Corollary 8.1.1. *If a has order k modulo n, then the integers $a, a^2, \ldots, a^k$ are incongruent modulo n.*

Proof. If $a^i \equiv a^j \pmod{n}$ for $1 \leq i \leq j \leq k$, then the theorem ensures that $i \equiv j \pmod{k}$. But this is impossible unless $i = j$. □

Theorem 8.1.3. *If the integer a has order k modulo n and $h > 0$, then a^h has order $k/\gcd(h, k)$ modulo n.*

Proof. Let $d = \gcd(h, k)$. Then we may write $h = h_1 d$ and $k = k_1 d$, with $\gcd(h_1, k_1) = 1$. Clearly,

$$(a^h)^{k_1} = (a^{h_1 d})^{k/d} = (a^k)^{h_1} \equiv 1 \pmod{n}.$$

If a^h is assumed to have order r modulo n, then Theorem 8.1.1 asserts that $r \mid k_1$. On the other hand, because a has order k modulo n, the congruence

$$a^{hr} \equiv (a^h)^r \equiv 1 \pmod{n}$$

indicates that $k \mid hr$; in other words, $k_1 d \mid h_1 dr$ or $k_1 \mid h_1 r$. But $\gcd(k_1, h_1) = 1$, and therefore $k_1 \mid r$. This divisibility relation, when combined with the one obtained earlier, gives

$$r = k_1 = \frac{k}{d} = \frac{k}{\gcd(h,k)},$$

proving the theorem. □

Corollary 8.1.2. *Let a have order k modulo n. Then a^h also has order k if and only if $\gcd(h,k) = 1$.*

Example 2. List the orders modulo 13 of the positive integers less than 13, and then illustrate the preceding theorem by identifying the integers that have order 12 modulo 13.

Definition 8.1.2. If $\gcd(a,n) = 1$ and a is of order $\phi(n)$ modulo n, then a is a primitive root of the integer n.

Example 3. Show that if $F_n = 2^{2^n} + 1$, $n > 1$, is a prime, then 2 is not a primitive root of F_n.

Theorem 8.1.4. *Let $\gcd(a,n) = 1$ and let $a_1, a_2, \ldots, a_{\phi(n)}$ be the positive integers less than n and relatively prime to n. If a is a primitive root of n, then*

$$a, a^2, \ldots, a^{\phi(n)}$$

are congruent modulo n to $a_1, a_2, \ldots, a_{\phi(n)}$, in some order.

Proof. Because a is relatively prime to n, the same holds for all the powers of a; hence, each a^k is congruent modulo n some one of the a_i. The $\phi(n)$ numbers in the set $\{a, a^2, \ldots, a^{\phi(n)}$ are incongruent by Corollary 8.1.1; thus, these powers must represent (not necessarily in order of appearance) the integers $a_1, a_2, \ldots, a_{\phi(n)}$. □

Corollary 8.1.3. *If n has a primitive root, then it has exactly $\phi(\phi(n))$ of them.*

Proof. Suppose that a is a primitive root of n. By the theorem, any other primitive root of n is found among the members of the set $\{a, a^2, \ldots, a^{\phi(n)}$. But the number of powers a^k, $1 \leq k \leq \phi(n)$, that have order $\phi(n)$ is equal to the number of integers k for which $\gcd(k, \phi(n)) = 1$; there are $\phi(\phi(n))$ such integers, hence $\phi(\phi(n))$ primitive roots of n. □

Example 4. Let r be a primitive root of the integer n. Prove that r^k is a primitive root of n if and only if $\gcd(k, \phi(n)) = 1$.

8.2 Primitive Roots for Primes

Theorem 8.2.1 (Lagrange)**.** *If p is a prime and*

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \qquad a_n \not\equiv 0 \pmod{p}$$

is a polynomial of degree $n \geq 1$ with integral coefficients, then the congruence

$$f(x) \equiv 0 \pmod{p}$$

has at most n incongruent solutions modulo p.

Proof. We proceed by induction on n, the degree of $f(x)$. If $n = 1$, then our polynomial is of the form

$$f(x) = a_1 x + a_0.$$

Because $\gcd(a_1, p) = 1$, Theorem 4.4.1 asserts that the congruence $a_1 x \equiv -a_0 \pmod{p}$ has a unique solution modulo p. Thus, the theorem holds for $n = 1$.

Now assume inductively that the theorem is true for polynomials of degree $k-1$, and consider the case in which $f(x)$ has degree k. Either the congruence $f(x) \equiv 0 \pmod{p}$ has no solutions (and we are finished), or it has at least one solution, call it a. If $f(x)$ is divided by $x - a$, the result is

$$f(x) = (x - a)q(x) + r$$

in which $q(x)$ is a polynomial of degree $k - 1$ with integral coefficients and r is an integer. Substituting $x = a$, we obtain

$$0 \equiv f(a) = (a - a)q(a) + r = r \pmod{p}$$

and therefore $f(x) \equiv (x - a)q(x) \pmod{p}$.

If b is another one of the incongruent solutions of $f(x) \equiv 0 \pmod{p}$, then

$$0 \equiv f(b) \equiv (b - a)q(b) \pmod{p}.$$

Because $b - a \not\equiv 0 \pmod{p}$, we may cancel to conclude that $q(b) \equiv 0 \pmod{p}$; in other words, any solution of $f(x) \equiv 0 \pmod{p}$ that is different from a must satisfy $q(x) \equiv 0 \pmod{p}$. By our induction assumption, the latter congruence can possess at most $k-1$ incongruent solutions, and therefore $f(x) \equiv 0 \pmod{p}$ has no more than k incongruent solutions. This completes the induction step and the proof. □

Corollary 8.2.1. *If p is a prime number and $d \mid p - 1$, then the congruence*

$$x^d - 1 \equiv 0 \pmod{p}$$

has exactly d solutions.

Proof. Because $d \mid p-1$, we have $p-1 = dk$ for some k. Then

$$x^{p-1} - 1 = (x^d - 1)f(x)$$

where the polynomial $f(x) = x^{d(k-1)} + x^{d(k-2)} + \cdots + x^d + 1$ has integral coefficients and is of degree $d(k-1) = p-1-d$. By Lagrange's theorem, the congruence $f(x) \equiv 0 \pmod{p}$ has at most $p-1-d$ solutions. We also know from Fermat's theorem that $x^{p-1} - 1 \equiv 0 \pmod{p}$ has precisely $p-1$ incongruent solutions; namely, the integers $1, 2, \ldots, p-1$.

Now any solution $x \equiv a \pmod{p}$ of $x^{p-1} - 1 \equiv 0 \pmod{p}$ that is not a solution of $f(x) \equiv 0 \pmod{p}$ must satisfy $x^d - 1 \equiv 0 \pmod{p}$. For

$$0 \equiv a^{p-1} - 1 = (a^d - 1)f(a) \pmod{p}$$

with $p \nmid f(a)$, implies that $p \mid a^d - 1$. It follows that $x^d - 1 \equiv 0 \pmod{p}$ must have at least

$$p - 1 - (p - 1 - d) = d$$

solutions. This last congruence can possess no more than d solutions by Lagrange's theorem and, hence, has exactly d solutions. □

Example 1. If p is an odd prime, prove the following:

(a) The only congruent solutions of $x^2 \equiv 1 \pmod{p}$ are 1 and $p-1$.

(b) The congruence $x^{p-2} + \cdots + x^2 + x + 1 \equiv 0 \pmod{p}$ has exactly $p-2$ incongruent solutions, and they are the integers $2, 3, \ldots, p-1$.

Theorem 8.2.2. *If p is a prime number and $d \mid p-1$, then there are exactly $\phi(d)$ incongruent integers having order d modulo p.*

Proof. Let $d \mid p-1$ and $\psi(d)$ denote the number of integers k, $1 \leq k \leq p-1$, that have order d modulo p. Because each integer between 1 and $p-1$ has order d for some $d \mid p-1$,

$$p-1 = \sum_{d|p-1} \psi(d).$$

At the same time, Gauss's theorem tells us that

$$p-1 = \sum_{d|p-1} \phi(d),$$

and therefore, putting these together,

$$\sum_{d|p-1} \psi(d) = \sum_{d|p-1} \phi(d). \tag{1}$$

Our aim is to show that $\psi(d) \leq \phi(d)$ for each divisor d of $p-1$, because this, in conjunction with equation (1), would produce the equality $\psi(d) = \phi(d) \neq 0$ (otherwise, the first sum would be strictly smaller than the second).

Given an arbitrary divisor d of $p-1$, there are two possibilities: we either have $\psi(d) = 0$ or $\psi(d) > 0$. If $\psi(d) = 0$, then certainly $\psi(d) \leq \phi(d)$. Suppose that $\psi(d) > 0$, so there exists an integer a of order d. Then the d integers $a, a^2, \ldots, a^d$ are incongruent modulo p and each of them satisfies the polynomial congruence

$$x^d - 1 \equiv 0 \pmod{p} \tag{2}$$

for, $(a^k)^d \equiv (a^d)^k \equiv 1 \pmod{p}$. By Corollary 8.2.1, there can be no other solutions of equation (2). It follows that any integer having order d modulo p must be congruent to one of $a, a^2, \ldots, a^d$. But only $\phi(d)$ of the just-mentioned powers have order d, namely those a^k for which the exponent k has the property $\gcd(k, d) = 1$. Hence, in the present situation $\psi(d) = \phi(d)$, and the number of integers having order d modulo p is equal to $\psi(d)$. □

Corollary 8.2.2. *If p is a prime, then there are exactly $\phi(p-1)$ incongruent primitive roots of p.*

Example 2. Find the $\phi(6) = 2$ integers having order 6 modulo 31.

Example 3. If p is a prime, show that the product of the $\phi(p-1)$ primitive roots of p is congruent modulo p to $(-1)^{\phi(p-1)}$.

8.3 Composite Numbers Having Primitive Roots

Theorem 8.3.1. *For $k \geq 3$, the integer 2^k has no primitive roots.*

Proof. We start by showing that if a is an odd integer, then for $k \geq 3$

$$a^{2^{k-2}} \equiv 1 \pmod{2^k}.$$

If $k = 3$, this congruence becomes $a^2 \equiv 1 \pmod 8$, which is certainly true (indeed, $1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \pmod 8$). For $k > 3$, we proceed by induction on k. Assume that the asserted congruence holds for the integer k; that is, $a^{2^{k-2}} \equiv 1 \pmod{2^k}$. This is equivalent to the equation

$$a^{2^{k-2}} = 1 + b2^k$$

where b is an integer. Squaring both sides, we obtain

$$\begin{aligned} a^{2^{k-1}} = (a^{2^{k-2}})^2 &= 1 + 2(b2^k) + (b2^k)^2 \\ &= 1 + 2^{k+1}(b + b^2 2^{k-1}) \\ &\equiv 1 \pmod{2^{k+1}}, \end{aligned}$$

so that the asserted congruence holds for $k + 1$ and, hence, for all $k \geq 3$.

Now the integers that are relatively prime to 2^k are precisely the odd integers, so that $\phi(2^k) = 2^{k-1}$. By what was just proved, if a is an odd integer and $k \geq 3$,

$$a^{\phi(2^k)/2} \equiv 1 \pmod{2^k}$$

and, consequently, there are no primitive roots of 2^k. □

Theorem 8.3.2. *If $\gcd(m, n) = 1$, where $m > 2$ and $n > 2$, the integer mn has no primitive roots.*

Proof. Consider any integer a for which $\gcd(a, mn) = 1$; then $\gcd(a, m) = 1$ and $\gcd(a, n) = 1$. Put $h = \operatorname{lcm}(\phi(m), \phi(n))$ and $d = \gcd(\phi(m), \phi(n))$.

Because $\phi(m)$ and $\phi(n)$ are both even (Theorem 7.2.4), surely $d \geq 2$. In consequence,

$$h = \frac{\phi(m)\phi(n)}{d} \leq \frac{\phi(mn)}{2}.$$

Now Euler's theorem asserts that $a^{\phi(m)} \equiv 1 \pmod m$. Raising this congruence to the $\phi(n)/d$ power, we get

$$a^h = (a^{\phi(m)})^{\phi(n)/d} \equiv 1^{\phi(n)/d} \equiv 1 \pmod m.$$

Similar reasoning leads to $a^h \equiv 1 \pmod{n}$. Together with the hypothesis $\gcd(m, n) = 1$, these congruences force the conclusion that

$$a^h \equiv 1 \pmod{mn}.$$

Therefore the order of any integer relatively prime to mn does not exceed $\phi(mn)/2$, whence there can be no primitive roots for mn. □

Corollary 8.3.1. *The integer n fails to have a primitive root if either*

(a) *n is divisible by two odd primes, or*

(b) *n is of the form $n = p^m p^k$, where p is an odd prime and $m \geq 2$.*

Example 1. if r is a primitive root of p^2, p being an odd prime, show that the solutions of the congruence $x^{p-1} \equiv 1 \pmod{p^2}$ are precisely the integers $r^p, r^{2p}, \ldots, r^{(p-1)p}$.

***Lemma* 8.3.1:** If p is an odd prime, then there exists a primitive root r of p such that $r^{p-1} \not\equiv 1 \pmod{p^2}$.

Proof. From Theorem 8.2.2, it is known that p has primitive roots. Choose one, and call it r. If $r^{p-1} \not\equiv 1 \pmod{p^2}$, then we are finished. In the contrary case, replace r by $r' = r+p$, which is also a primitive root of p. Then employing the binomial theorem,

$$(r')^{p-1} \equiv (r+p)^{p-1} \equiv r^{p-1} + (p-1)pr^{p-2} \pmod{p^2}.$$

But we have assumed that $r^{p-1} \equiv 1 \pmod{p^2}$; hence,

$$(r')^{p-1} \equiv 1 - pr^{p-2} \pmod{p^2}.$$

Because r is a primitive root of p, $\gcd(r,p) = 1$, and therefore $p \nmid r^{p-2}$. The outcome of all this is that $(r')^{p-1} \not\equiv 1 \pmod{p^2}$. □

Corollary 8.3.2. *If p is an odd prime, then p^2 has a primitive root; in fact, for a primitive root r of p, either r or $r+p$ (or both) is a primitive root of p^2.*

Proof. If r is a primitive root of p, then the order of r modulo p^2 is either $p-1$ or $p(p-1) = \phi(p^2)$. The foregoing proof shows that if r has order $p-1$ modulo p^2, then $r+p$ is a primitive root of p^2. □

***Lemma* 8.3.2:** Let p be an odd prime and let r be a primitive root of p with the property that $r^{p-1} \not\equiv 1 \pmod{p^2}$. Then for each positive integer $k \geq 2$,

$$r^{p^{k-2}(p-1)} \not\equiv 1 \pmod{p^k}.$$

Proof. The proof proceeds by induction on k. By hypothesis, the assertion holds for $k = 2$. Let us assume that it is true for some $k \geq 2$ and show that it is true for $k+1$. Because $\gcd(r, p^{k-1}) = \gcd(r, p^k) = 1$, Euler's theorem indicates that

$$r^{p^{k-2}(p-1)} = r^{\phi(p^{k-1})} \equiv 1 \pmod{p^k}.$$

Hence, there exists an integer a satisfying

$$r^{p^{k-2}(p-1)} = 1 + ap^{k-1}$$

where $p \nmid a$ by our induction hypothesis. Raise both sides of this last equation to the pth power and expand to obtain

$$r^{p^{k-1}(p-1)} = (1 + ap^{k-1})^p \equiv 1 + ap^k \pmod{p^{k+1}}.$$

Because the integer a is not divisible by p, we have

$$r^{p^{k-1}(p-1)} \not\equiv 1 \pmod{p^{k+1}}.$$

This completes the induction step, thereby proving the lemma. □

Theorem 8.3.3. *If p is an odd prime number and $k \geq 1$, then there exists a primitive root for p^k.*

Proof. The two lemmas allow us to choose a primitive root r of p for which $r^{p^{k-2}(p-1)} \not\equiv 1 \pmod{p^k}$; in fact, any integer r satisfying the condition $r^{p-1} \not\equiv 1 \pmod{p^2}$ will do. We argue that such an r serves as a primitive root for all powers of p.

Let n be the order of r modulo p^k. In compliance with Theorem 8.1.1, n must divide $\phi(p^k) = p^{k-1}(p-1)$. Because $r^n \equiv 1 \pmod{p^k}$ yields $r^n \equiv 1 \pmod{p}$, we also have $p - 1 \mid n$. Consequently, n assumes the form $n = p^m(p-1)$, where $0 \leq m \leq k-1$. If it happened that $n \neq p^{k-1}(p-1)$, then $p^{k-2}(p-1)$ would be divisible by n and we would arrive at

$$r^{p^{k-2}(p-1)} \equiv 1 \pmod{p^k},$$

contradicting the way in which r was initially chosen. Therefore, $n = p^{k-1}(p-1)$ and r is a primitive root for p^k. □

Corollary 8.3.3. *There are primitive roots for $2p^k$, where p is an odd prime and $k \geq 1$.*

Proof. Let r be a primitive root for p^k. There is no harm in assuming that r is an odd integer; for, if it is even, then $r + p^k$ is odd and is still a primitive root for p^k. Then $\gcd(r, 2p^k) = 1$. The order n of r modulo $2p^k$ must divide

$$\phi(2p^k) = \phi(2)\phi(p^k) = \phi(p^k).$$

But $r^n \equiv 1 \pmod{2p^k}$ implies that $r^n \equiv 1 \pmod{p^k}$, and therefore $\phi(p^k) \mid n$. Together these divisibility conditions force $n = \phi(2p^k)$, making r a primitive root of $2p^k$. □

Theorem 8.3.4. *An integer $n > 1$ has a primitive root if and only if*

$$n = 2, 4, p^k, \text{ or } 2p^k$$

where p is an odd prime.

Proof. By virtue of Theorems 8.3.1 and 8.3.2, the only positive integers with primitive roots are those mentioned in the statement of our theorem. It may be checked that 1 is a primitive root for 2, and 3 is a primitive root of 4. We have just finished proving that primitive roots exist for any power of an odd prime and for twice such a power. □

Example 2. Assume that r is a primitive root of the odd prime p and $(r + tp)^{p-1} \not\equiv 1 \pmod{p^2}$. Show that $r + tp$ is a primitive root of p^k for each $k \geq 1$.

8.4 The Theory of Indices

Definition 8.4.1. Let r be a primitive root of n. if $\gcd(a, n) = 1$, then the smallest positive integer k such that $a \equiv r^k \pmod{n}$ is called the index of a relative to r.

Theorem 8.4.1. *If n has a primitive root r and $\operatorname{ind} a$ denotes the index of a relative to r, then the following properties hold:*

(a) $\operatorname{ind}(ab) \equiv \operatorname{ind} a + \operatorname{ind} b \pmod{\phi(n)}$.

(b) $\operatorname{ind} a^k \equiv k \operatorname{ind} a \pmod{\phi(n)}$ *for* $k > 0$.

(c) $\operatorname{ind} 1 \equiv 0 \pmod{\phi(n)}$, $\operatorname{ind} r \equiv 1 \pmod{\phi(n)}$.

Proof. By the definition of index, $r^{\operatorname{ind} a} \equiv a \pmod{n}$ and $r^{\operatorname{ind} b} \equiv b \pmod{n}$. Multiplying these congruences together, we obtain

$$r^{\operatorname{ind} a + \operatorname{ind} b} \equiv ab \pmod{n}.$$

But $r^{\operatorname{ind}(ab)} \equiv ab \pmod{n}$, so that

$$r^{\operatorname{ind} a + \operatorname{ind} b} \equiv r^{\operatorname{ind}(ab)} \pmod{n}.$$

It may very well happen that $\operatorname{ind} a + \operatorname{ind} b$ exceeds $\phi(n)$. This presents no problem, for Theorem 8.1.2 guarantees that the last equation holds if and only if the exponents are congruent modulo $\phi(n)$; that is,

$$\operatorname{ind} a + \operatorname{ind} b = \operatorname{ind}(ab) \pmod{\phi(n)},$$

which is property (a).

The proof of property (b) proceeds along much the same lines. For we have $r^{\operatorname{ind} a^k} \equiv a^k \pmod{n}$, and by the laws of exponents, $r^{k \operatorname{ind} a} = (r^{\operatorname{ind} a})^k \equiv a^k \pmod{n}$; hence,

$$r^{\operatorname{ind} a^k} \equiv r^{k \operatorname{ind} a} \pmod{n}.$$

As above, the implication is that $\operatorname{ind} a^k \equiv k \operatorname{ind} a \pmod{\phi(n)}$. The two parts of property (c) should be fairly apparent. □

Example 1. Solve the congruence

$$4x^9 \equiv 7 \pmod{13}.$$

Theorem 8.4.2. *Let n be an integer possessing a primitive root and let $\gcd(a, n) = 1$. Then the congruence $x^k \equiv a \pmod{n}$ has a solution if and only if*

$$a^{\phi(n)/d} \equiv 1 \pmod{n}$$

where $d = \gcd(k, \phi(n))$; if it has a solution, there are exactly d solutions modulo n.

Proof. Taking indices, the congruence $a^{\phi(n)/d} \equiv 1 \pmod{n}$ is equivalent to

$$\frac{\phi(n)}{d} \operatorname{ind} a \equiv 0 \pmod{\phi(n)},$$

which, in turn, holds if and only if $d \mid \operatorname{ind} a$. But we have just seen that the latter is a necessary and sufficient condition for the congruence $x^k \equiv a \pmod{n}$ to be solvable. □

Corollary 8.4.1. *Let p be a prime and $\gcd(a, p) = 1$. Then the congruence $x^k \equiv a \pmod{p}$ has a solution if and only if $a^{(p-1)/d} \equiv 1 \pmod{p}$, where $d = \gcd(k, p - 1)$.*

Example 2. Is the congruence $x^3 \equiv 4 \pmod{13}$ solvable? What about $x^3 \equiv 5 \pmod{13}$?

Example 3. Find the remainder when $3^{24} \cdot 5^{13}$ is divided by 17.

Example 4. Let r be a primitive root of the odd prime p, and let $d = \gcd(k, p-1)$. Prove that the values of a for which the congruence $x^k \equiv a \pmod{p}$ is solvable are $r^d, r^{2d}, \ldots, r^{[(p-1)/d]d}$.

Chapter 9

The Quadratic and Reciprocity Law

9.1 Euler's Criterion

Definition 9.1.1. Let p be an odd prime and $\gcd(a, p) = 1$. If the quadratic congruence $x^2 \equiv a \pmod{p}$ has a solution, then a is said to be a quadratic residue of p. Otherwise, a is called a quadratic nonresidue of p.

Example 1. Find the quadratic residues of the prime $p = 13$.

Theorem 9.1.1 (Euler's criterion)**.** *Let p be an odd prime and $\gcd(a, p) = 1$. Then a is a quadratic residue of p if and only if $a^{(p-1)/2} \equiv 1 \pmod{p}$.*

Proof. Suppose that a is a quadratic residue of p, so that $x^2 \equiv a \pmod{p}$ admits a solution, call it x_1. Because $\gcd(a, p) = 1$, evidently $\gcd(x_1, p) = 1$.

We may therefore appeal to Fermat's theorem to obtain

$$a^{(p-2)/2} \equiv (x_1^2)^{(p-1)/2} \equiv x_1^{p-1} \equiv 1 \pmod{p}.$$

For the opposite direction, assume that the congruence $a^{(p-1)/2} \equiv 1 \pmod{p}$ holds and let r be a primitive root of p. Then $a \equiv r^k \pmod{p}$ for some integer k, with $1 \leq k \leq p-1$. It follows that

$$r^{k(p-1)/2} \equiv a^{(p-1)/2} \equiv 1 \pmod{p}.$$

By Theorem 8.1.1, the order of r (namely, $p-1$) must divide the exponent $k(p-1)/2$. The implication is that k is an even integer, say $k = 2j$. Hence,

$$(r^j)^2 = r^{2j} = r^k \equiv a \pmod{p},$$

making the integer r^j a solution of the congruence $x^2 \equiv a \pmod{p}$. This proves that a is a quadratic residue of the prime p. □

Corollary 9.1.1. *Let p be an odd prime and $\gcd(a, p) = 1$. Then a is a quadratic residue or nonresidue of p according to whether*

$$a^{(p-1)/2} \equiv 1 \pmod{p} \quad \textit{or} \quad a^{(p-1)/2} \equiv -1 \pmod{p}.$$

Proof. If p is an odd prime and $\gcd(a, p) = 1$, then

$$(a^{(p-1)/2} - 1)(a^{(p-1)/2} + 1) = a^{p-1} - 1 \equiv 0 \pmod{p},$$

the last congruence being justified by Fermat's theorem. Hence, either

$$a^{(p-1)/2} \equiv 1 \pmod{p} \quad \text{or} \quad a^{(p-1)/2} \equiv -1 \pmod{p}.$$

but not both. For, if both congruences held simultaneously, then we would have $1 \equiv -1 \pmod{p}$, or equivalently, $p \mid 2$, which conflicts with our hypothesis. Because a quadratic residue of P does not satisfy $a^{(p-1)/2} \equiv 1 \pmod{p}$, it must therefore satisfy $a^{(p-1)/2} \equiv -1 \pmod{p}$. □

Example 2. Determine whether the integers 2 and 3 are quadratic residues of $p = 13$.

Example 3. Prove that the quadratic congruence $6x^2 + 5x + 1 \equiv 0 \pmod{p}$ has a solution for every prime p, even though the equation $6x^2 + 5x + 1 = 0$ has no solution in the integers.

Example 4. If $p = 2^k + 1$ is prime, verify that every quadratic nonresidue of p is a primitive root of p.

9.2 The Legendre Symbol and its Properties

Definition 9.2.1. Let p be an odd prime and let $\gcd(a, p) = 1$. The Legendre symbol (a/p) is defined by

$$(a/p) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue of } p \\ -1 & \text{if } a \text{ is a quadratic nonresidue of } p. \end{cases}$$

We shall refer to a as the numerator and p as the denominator of the symbol (a/p). Another standard notation for the Legendre symbol is $(\frac{a}{p})$ or $(a \mid p)$.

Example 1. Illustrate the definition of the Legendre symbol using $p = 13$.

Remark 1. For $p \mid a$, we have purposely left the symbol (a/p) undefined. Some authors find it convenient to extend Legendre's definition to this case by setting $(a/p) = 0$. One advantage of this is that the number of solutions of $x^2 \equiv a \pmod{p}$ can then be given by the simple formula $1 + (a/p)$.

Theorem 9.2.1. *Let p be an odd prime and let a and b be integers that are relatively prime to p. Then the Legendre symbol has the following properties:*

(a) *If $a \equiv b \pmod{p}$, then $(a/p) = (b/p)$.*

(b) $(a^2/p) = 1$.

(c) $(a/p) \equiv a^{(p-1)/2} \pmod{p}$.

(d) $(ab/p) = (a/p)(b/p)$.

(e) $(1/p) = 1$ *and* $(-1/p) = (-1)^{(p-1)/2}$.

Proof. If $a \equiv b \pmod{p}$, then the two congruences $x^2 \equiv a \pmod{p}$ and $x^2 \equiv b \pmod{p}$ have exactly the same solutions, if any at all. Thus, $x^2 \equiv a \pmod{p}$ and $x^2 \equiv b \pmod{p}$ are both solvable, or neither one has a solution. This is reflected in the statement $(a/p) = (b/p)$.

Regarding property (b), observe that the integer a trivially satisfies the congruence $x^2 \equiv a^2 \pmod{p}$; hence, $(a^2/p) = 1$. Property (c) is just the

corollary to Theorem 9.1.1 rephrased in terms of the Legendre symbol. We use (c) to establish property (d):

$$(ab/p) \equiv (ab)^{(p-1)/2} \equiv a^{(p-1)/2}b^{(p-1)/2} \equiv (a/p)(b/p) \pmod{p}.$$

Now the Legendre symbol assumes only the values 1 or -1. If $(ab/p) \neq (a/p)(b/p)$, we would have $1 \equiv -1 \pmod{p}$ or $2 \equiv 0 \pmod{p}$; this cannot occur, because $p > 2$. It follows that

$$(ab/p) = (a/p)(b/p).$$

Finally, we observe that the first equality in property (e) is a special case of property (b), whereas the second one is obtained from property (c) upon setting $a = -1$. Because the quantities $(-1/p)$ and $(-1)^{(p-1)/2}$ are either 1 or -1, the resulting congruence

$$(-1/p) \equiv (-1)^{(p-1)/2} \pmod{p}$$

implies that $(-1/p) = (-1)^{(p-1)/2}$. □

Corollary 9.2.1. *If p is an odd prime, then*

$$(-1/p) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{4} \\ -1 & \text{if } p \equiv 3 \pmod{4}. \end{cases}$$

Example 2. Determine whether the congruence $x^2 \equiv -46 \pmod{17}$ is solvable.

Theorem 9.2.2. *There are infinitely many primes of the form $4k + 1$.*

Proof. Suppose that there are finitely many such primes; let us call them $p_1, p_2, \ldots, p_n$ and consider the integer

$$N = (2p_1p_2 \cdots p_n)^2 + 1.$$

Clearly N is odd, so that there exists some odd prime p with $p \mid N$. To put it another way,

$$(2p_1p_2 \cdots p_n)^2 \equiv -1 \pmod{p}$$

or, if we prefer to phrase this in terms of the Legendre symbol, $(-1/p) = 1$. But the relation $(-1/p) = 1$ holds only if p is of the form $4k + 1$. Hence, p is one of the primes p_i, implying that p_i divides $N - (2p_1p_2 \cdots p_n)^2$, or $p_i \mid 1$, which is a contradiction. □

Theorem 9.2.3. *If p is an odd prime, then*

$$\sum_{a=1}^{p-1}(a/p) = 0.$$

Hence, there are precisely $(p-1)/2$ quadratic residues and $(p-1)/2$ quadratic nonresidues of p.

Proof. Let r be a primitive root of p. We know that, modulo p, the powers $r, r^2, \ldots, r^{p-1}$ are just a permutation of the integers $1, 2, \ldots, p-1$. Thus, for any a lying between 1 and $p-1$, inclusive, there exists a unique positive integer k $(1 \leq k \leq p-1)$, such that $a \equiv r^k \pmod{p}$. By appropriate use of Euler's criterion, we have

$$(a/p) = (r^k/p) \equiv (r^k)^{(p-1)/2} = (r^{(p-1)/2})^k \equiv (-1)^k \pmod{p} \qquad (1)$$

where, because r is a primitive root of p, $r^{(p-1)/2} \equiv -1 \pmod{p}$. But (a/p) and $(-1)^k$ are equal to either 1 or -1, so that equality holds in equation (1). Now add up the Legendre symbols in question to obtain

$$\sum_{a=1}^{p-1}(a/p) = \sum_{k=1}^{p-1}(-1)^k = 0.$$ □

Corollary 9.2.2. *The quadratic residues of an odd prime p are congruent modulo p to the even powers of a primitive root r of p; the quadratic nonresidues are congruent to the odd powers of r.*

Example 3. For an odd prime p, prove that there are $(p-1)/2 - \phi(p-1)$ quadratic nonresidues of p that are not primitive roots of p.

Theorem 9.2.4 (Gauss's lemma)**.** *Let p be an odd prime and let* $\gcd(a,p) = 1$. *If n denotes the number of integers in the set*

$$S = \left\{ a, 2a, 3a, \ldots, \left(\frac{p-1}{2}\right) a \right\}$$

whose remainders upon division by p exceed $p/2$, then

$$(a/p) = (-1)^n.$$

Proof. Because $\gcd(a,p) = 1$, none of the $(p-1)/2$ integers in S is congruent to zero and no two are congruent to each other modulo p. Let $r_1, \ldots, r_m$ be those remainders upon division by p such that $0 < r_i < p/2$, and let $s_1, \ldots, s_n$ be those remainders such that $p > s_i > p/2$. Then $m+n = (p-1)/2$, and the integers

$$r_1, \ldots, r_m \qquad p - s_1, \ldots, p - s_n$$

are all positive and less than $p/2$.

To prove that these integers are all distinct, it suffices to show that no $p - s_i$ is equal to any r_j. Assume to the contrary that

$$p - s_i = r_j$$

for some choice of i and j. Then there exist integers u and v, with $1 \leq u, v \leq (p-1)/2$, satisfying $s_i \equiv ua \pmod{p}$ and $r_j \equiv va \pmod{p}$. Hence,

$$(u+v)a \equiv s_i + r_j = p \equiv 0 \pmod{p},$$

which says that $u + v \equiv 0 \pmod{p}$. But the latter congruence cannot take place, because $1 < u + v \leq p - 1$.

The point we wish to bring out is that the $(p-1)/2$ numbers

$$r_1, \ldots, r_m \qquad p - s_1, \ldots, p - s_n$$

are simply the integers $1, 2, \ldots, (p-1)/2$, not necessarily in order of appearance. Thus, their product is $[(p-1)/2]!$:

$$\begin{aligned}\left(\frac{p-1}{2}\right)! &= r_1 \cdots r_m (p - s_1) \cdots (p - s_n) \\ &\equiv r_1 \cdots r_m (-s_1) \cdots (-s_n) \pmod{p} \\ &\equiv (-1)^n r_1 \cdots r_m s_1 \cdots s_n \pmod{p}.\end{aligned}$$

But we know that $r_1, \ldots, r_m, s_1, \ldots, s_n$ are congruent modulo p to $a, 2a, \ldots, [(p-1)/2]a$, in some order, so that

$$\begin{aligned}\left(\frac{p-1}{2}\right)! &= (-1)^n a \cdot 2a \cdots \left(\frac{p-1}{2}\right) a \pmod{p} \\ &\equiv (-1)^n a^{(p-1)/2} \left(\frac{p-1}{2}\right)! \pmod{p}.\end{aligned}$$

Because $[(p-1)/2]!$ is relatively prime to p, it may be canceled from both sides of this congruence to give

$$1 \equiv (-1)^n a^{(p-1)/2} \pmod{p}$$

or, upon multiplying by $(-1)^n$,

$$a^{(p-1)/2} \equiv (-1)^n \pmod{p}.$$

Use of Euler's criterion now completes the argument:

$$(a/p) \equiv a^{(p-1)/2} \equiv (-1)^n \pmod{p},$$

which implies that

$$(a/p) = (-1)^n. \qquad \square$$

Theorem 9.2.5. *If p is an odd prime, then*

$$(2/p) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 8 \text{ or } p \equiv 7 \pmod 8 \\ -1 & \text{if } p \equiv 3 \pmod 8 \text{ or } p \equiv 5 \pmod 8. \end{cases}$$

Proof. According to Gauss's lemma, $(2/p) = (-1)^n$, where n is the number of integers in the set

$$S = \left\{1 \cdot 2, 2 \cdot 2, 3 \cdot 2, \ldots, \left(\frac{p-1}{2}\right) \cdot 2\right\}$$

which, upon division by p, have remainders greater than $p/2$. The members of S are all less than p, so that it suffices to count the number that exceed $p/2$. For $1 \leq k \leq (p-1)/2$, we have $2k < p/2$ if and only if $k < p/4$. If $[\ ]$ denotes the greatest integer function, then there are $[p/4]$ integers in S less than $p/2$; hence,

$$n = \frac{p-1}{2} - \left[\frac{p}{4}\right]$$

is the number of integers that are greater than $p/2$.

Now we have four possibilities, for any odd prime has one of the forms $8k+1$, $8k+3$, $8k+5$, or $8k+7$. A simple calculation shows that

$$\begin{aligned}
&\text{if } p = 8k+1, \text{ then } n = 4k - \left[2k + \frac{1}{4}\right] = 4k - 2k = 2k \\
&\text{if } p = 8k+3, \text{ then } n = 4k + 1 - \left[2k + \frac{3}{4}\right] = 4k + 1 - 2k = 2k + 1 \\
&\text{if } p = 8k+5, \text{ then } n = 4k + 2 - \left[2k + 1 + \frac{1}{4}\right] \\
&\qquad\qquad = 4k + 2 - (2k+1) = 2k + 1 \\
&\text{if } p = 8k+7, \text{ then } n = 4k + 3 - \left[2k + 1 + \frac{3}{4}\right] \\
&\qquad\qquad = 4k + 3 - (2k+1) = 2k + 2.
\end{aligned}$$

Thus, when p is of the form $8k+1$ or $8k+7$, n is even and $(2/p) = 1$; on the other hand, when p assumes the form $8k+3$ or $8k+5$, n is odd and $(2/p) = -1$. □

Corollary 9.2.3. *If p is an odd prime, then*

$$(2/p) = (-1)^{(p^2-1)/8}.$$

Proof. If the prime p is of the form $8k \pm 1$ (equivalently, $p \equiv 1 \pmod 8$ or $p \equiv 7 \pmod 8$), then

$$\frac{p^2-1}{8} = \frac{(8k \pm 1)^2 - 1}{8} = \frac{64k^2 \pm 16k}{8} = 8k^2 \pm 2k,$$

which is an even integer; in this situation, $(-1)^{(p-1)/8} = 1 = (2/p)$. On the other hand, if p is of the form $8k \pm 3$ (equivalently, $p \equiv 3 \pmod 8$ or $p \equiv 5 \pmod 8$), then

$$\frac{p^2-1}{8} = \frac{(8k \pm 3)^2 - 1}{8} = \frac{64k^2 \pm 48k + 8}{8} = 8k^2 \pm 6k + 1,$$

which is odd; here, we have $(-1)^{(p^2-1)/8} = -1 = (2/p)$. □

Example 4. For a prime $p \equiv 7 \pmod 8$, show that $p \mid 2^{(p-1)/2} - 1$.

Example 5. Confirm that the numbers $2^n - 1$ are composite for $n = 11$, 23, 83, 131, 179, 183, 239, 251.

Theorem 9.2.6. *If p and $2p+1$ are both odd primes, then the integer $(-1)^{(p-1)/2}2$ is a primitive root of $2p+1$.*

Proof. For ease of discussion, let us put $q = 2p+1$. We distinguish two cases: $p \equiv 1 \pmod 4$ and $p \equiv 3 \pmod 4$. If $p \equiv 1 \pmod 4$, then $(-1)^{(p-1)/2}2 = 2$. Because $\phi(q) = q - 1 = 2p$, the order of 2 modulo q is one of the numbers 1, 2, p, or $2p$. Taking note of property (c) of Theorem 9.2.1, we have

$$(2/q) \equiv 2^{(q-1)/2} = 2^p \pmod q.$$

But, in the present setting, $q \equiv 3 \pmod 8$; whence, the Legendre symbol $(2/q) = -1$. It follows that $2^p = -1 \pmod q$, and therefore 2 cannot have order p modulo q. The order of 2 being neither 1, 2, ($2^2 \equiv 1 \pmod q$ implies that $q \mid 3$, which is an impossibility) nor p, we are forced to conclude that the order of 2 modulo q is $2p$. This makes 2 a primitive root of q.
We now deal with the case $p \equiv 3 \pmod 4$. This time, $(-1)^{(p-1)/2}2 = -2$ and

$$(-2)^p \equiv (-2/q) = (-1/q)(2/q) \pmod q.$$

Because $q \equiv 7 \pmod 8$, Corollary 9.2.1 asserts that $(-1/q) = -1$, whereas once again we have $(2/q) = 1$. This leads to the congruence $(-2)^p \equiv -1 \pmod q$. From here on, the argument duplicates that of the last paragraph. □

Theorem 9.2.7. *There are infinitely many primes of the form $8k-1$.*

Proof. As usual, suppose that there are only a finite number of such primes. Let these be $p_1, p_2, \ldots, p_n$ and consider the integer

$$N = (4p_1p_2 \cdots p_n)^2 - 2.$$

There exists at least one odd prime divisor p of N, so that

$$(4p_1p_2 \cdots p_n)^2 \equiv 2 \pmod p$$

or $(2/p) = 1$. In view of Theorem 9.2.5, $p \equiv \pm 1 \pmod 8$. If all the odd prime divisors of N were of the form $8k+1$, then N would be of the form $8a+1$; this is clearly impossible, because N is of the form $16a - 2$. Thus, N must have a prime divisor q of the form $8k-1$. But $q \mid N$, and $q \mid (4p_1p_2 \cdots p_n)^2$ leads to the contradiction that $q \mid 2$. □

***Lemma* 9.2.1:** If p is an odd prime and a an odd integer, with $\gcd(a, p) = 1$, then

$$(a/p) = (-1)^{\sum_{k=1}^{(p-1)/2}[ka/p]}.$$

Proof. Consider the set of integers

$$S = \left\{ a, 2a, 3a, \ldots, \left(\frac{p-1}{2}\right) a \right\}.$$

Divide each of these multiples of a by p to obtain

$$ka = q_k p + t_k \qquad 1 \leq t_k \leq p-1.$$

Then $ka/p = q_k + t_k/p$, so that $[ka/p] = q_k$. Thus, for $1 \leq k \leq (p-1)/2$, we may write ka in the form

$$ka = \left[\frac{ka}{p}\right] p + t_k. \tag{2}$$

If the remainder $t_k < p/2$, then it is one of the integers $r_1, \ldots, r_m$; on the other hand, if $t_k > p/2$, then it is one of the integers $s_1, \ldots, s_n$.

Taking the sum of the $(p-1)/2$ equations in equation (2), we get the relation

$$\sum_{k=1}^{(p-1)/2} ka = \sum_{k=1}^{(p-1)/2} \left[\frac{ka}{p}\right] p + \sum_{k=1}^{m} r_k + \sum_{k=1}^{n} s_k. \tag{3}$$

It was learned in proving Gauss's lemma that the $(p-1)/2$ numbers

$$r_1, \ldots, r_m \qquad p - s_1, \ldots, p - s_n$$

are just a rearrangement of the integers $1, 2, \ldots, (p-1)/2$. Hence

$$\sum_{k=1}^{(p-1)/2} k = \sum_{k=1}^{m} r_k + \sum_{k=1}^{n} (p - s_k) = pn + \sum_{k=1}^{m} r_k - \sum_{k=1}^{n} s_k. \tag{4}$$

Subtracting equation (4) from equation (3) gives

$$(a-1) \sum_{k=1}^{(p-1)/2} k = p \left(\sum_{k=1}^{(p-1)/2} \left[\frac{ka}{p}\right] - n \right) + 2 \sum_{k=1}^{n} s_k. \tag{5}$$

Let us use the fact that $p \equiv 1 \pmod 2$ and translate this last equation into a congruence modulo 2:

$$0 \cdot \sum_{k=1}^{(p-1)/2} k \equiv 1 \cdot \left(\sum_{k=1}^{(p-1)/2} \left[\frac{ka}{p}\right] - n \right) \pmod 2$$

or

$$n \equiv \sum_{k=1}^{(p-1)/2} \left[\frac{ka}{p}\right] \pmod 2.$$

The rest follows from Gauss's lemma; for,

$$(a/p) = (-1)^n = (-1)^{\sum_{k=1}^{(p-1)/2} [ka/p]}.$$ □

9.3 Quadratic Reciprocity

Theorem 9.3.1 (Quadratic Reciprocity Law)**.** *If p and q are distinct odd primes, then*

$$(p/q)(q/p) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

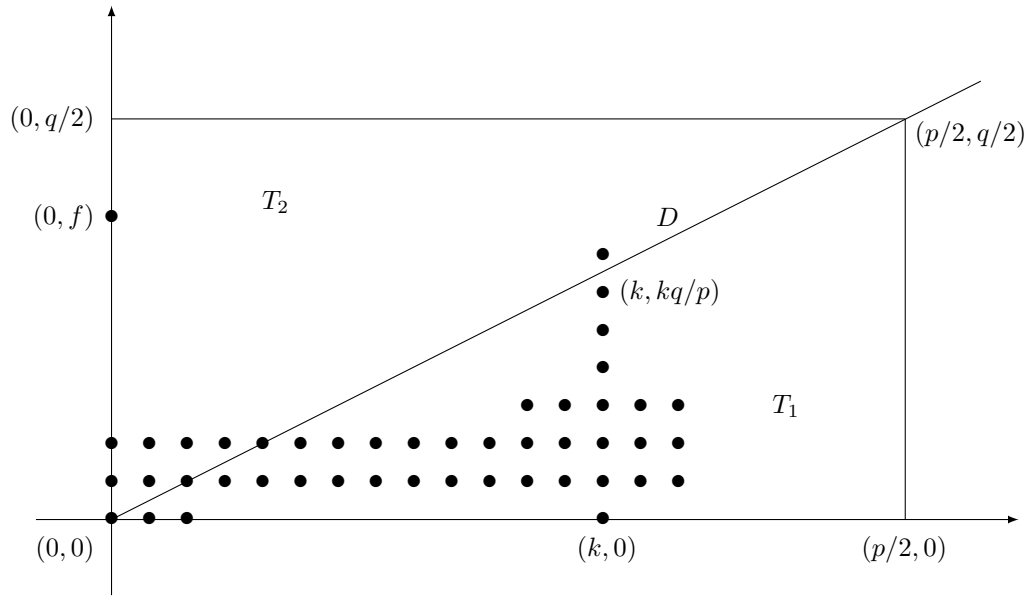
Proof. Consider the rectangle in the xy coordinate plane whose vertices are $(0,0)$, $(p/2,0)$, $(0,q/2)$, and $(p/2,q/2)$. Let R denote the region within this rectangle, not including any of the bounding lines. The general plan of attack is to count the number of lattice points (that is, the points whose coordinates are integers) inside R in two different ways. Because p and q are both odd, the lattice points in R consist of all points (n,m), where $1 \leq n \leq (p-1)/2$ and $1 \leq m \leq (q-1)/2$; clearly, the number of such points is

$$\frac{p-1}{2} \cdot \frac{q-1}{2}.$$

Now the diagonal D from $(0,0)$ to $(p/2,q/2)$ has the equation $y = (q/p)x$, or equivalently, $py = qx$. Because $\gcd(p,q) = 1$, none of the lattice points inside R will lie on D For p must divide the x coordinate of any lattice point on the line $py = qx$, and q must divide its y coordinate; there are no such points in R. Suppose that T_1 denotes the portion of R that is below the diagonal D, and T_2 the portion above. By what we have just seen, it suffices to count the lattice points inside each of these triangles.

The number of integers in the interval $0 < y < kq/p$ is equal to $[kq/p]$. Thus, for $1 \leq k \leq (p-1)/2$, there are precisely $[kq/p]$ lattice points in T_1 directly above the point $(k,0)$ and below D; in other words, lying on the vertical line segment from $(k,0)$ to $(k,kq/p)$. It follows that the total number of lattice points contained in T_1 is

$$\sum_{k=1}^{(p-1)/2} \left[\frac{kq}{p}\right].$$



A similar calculation, with the roles of p and q interchanged, shows that the number of lattice points within T_2 is

$$\sum_{j=1}^{(q-1)/2} \left[\frac{jp}{q}\right].$$

This accounts for all of the lattice points inside R, so that

$$\frac{p-1}{2} \cdot \frac{q-1}{2} = \sum_{k=1}^{(p-1)/2} \left[\frac{kq}{p}\right] + \sum_{j=1}^{(q-1)/2} \left[\frac{jp}{q}\right].$$

Finally, by Gauss's lemma,

$$\begin{aligned}(p/q)(q/p) &= (-1)^{\sum_{j=1}^{(q-1)/2}[jp/q]} \cdot (-1)^{\sum_{k=1}^{(p-1)/2}[kq/p]} \\ &= (-1)^{\sum_{j=1}^{(q-1)/2}[jp/q]+\sum_{k=1}^{(p-1)/2}[kq/p]} \\ &= (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.\end{aligned}$$

□

Corollary 9.3.1. *If p and q are distinct odd primes, then*

$$(p/q)(q/p) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4 \text{ or } q \equiv 1 \pmod 4 \\ -1 & \text{if } p \equiv q \equiv 3 \pmod 4. \end{cases}$$

Proof. The number $(p-1)/2 \cdot (q-1)/2$ is even if and only if at least one of the integers p and q is of the form $4k+1$; if both are of the form $4k+3$, then the product $(p-1)/2 \cdot (q-1)/2$ is odd. □

Corollary 9.3.2. *If p and q are distinct odd primes, then*

$$(p/q) = \begin{cases} (q/p) & \text{if } p \equiv 1 \pmod 4 \text{ or } q \equiv 1 \pmod 4 \\ -(q/p) & \text{if } p \equiv q \equiv 3 \pmod 4. \end{cases}$$

Example 1. Apply the preceding results to the Legendre symbol (29/53).

Theorem 9.3.2. *If $p \neq 3$ is an odd prime, then*

$$(3/p) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod{12} \\ -1 & \text{if } p \equiv \pm 5 \pmod{12}. \end{cases}$$

Proof. Because $3 \equiv 3 \pmod 4$, the preceding corollary implies that

$$(3/p) = \begin{cases} (p/3) & \text{if } p \equiv 1 \pmod 4 \\ -(p/3) & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

Now $p \equiv 1 \pmod 3$ or $p \equiv 2 \pmod 3$. By Theorems 9.2.1 and 9.2.5,

$$(p/3) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 3 \\ -1 & \text{if } p \equiv 2 \pmod 3), \end{cases}$$

the implication of which is that $(3/p) = 1$ if and only if

$$p \equiv 1 \pmod 4 \qquad \text{and} \qquad p \equiv 1 \pmod 3 \tag{1}$$

or

$$p \equiv 3 \pmod 4 \qquad \text{and} \qquad p \equiv 2 \pmod 3. \tag{2}$$

The restrictions in the congruencies in equation (1) are equivalent to requiring that $p \equiv 1 \pmod{12}$ whereas those congruencies in equation (2) are equivalent to $p \equiv 11 \equiv -1 \pmod{12}$. □

Example 2. Solve the quadratic congruence

$$x^2 \equiv 196 \pmod{1357}.$$

Example 3. If $F_n = 2^{2^n} + 1$, $n > 1$, is a prime, then 2 is not a primitive root of F_n. Show that the integer 3 serves as a primitive root of any prime of this type.

Example 4. Establish that 7 is a primitive root of any prime of the form $p = 2^{4n} + 1$.

9.4 Quadratic Congruences with Composite Moduli

Theorem 9.4.1. *If p is an odd prime and $\gcd(a, p) = 1$, then the congruence*

$$x^2 \equiv a \pmod{p^n} \qquad n \geq 1$$

has a solution if and only if $(a/p) = 1$.

Proof. If $x^2 \equiv a \pmod{p^n}$ has a solution, then so does $x^2 \equiv a \pmod{p}$—in fact, the same solution—whence $(a/p) = 1$.

For the converse, suppose that $(a/p) = 1$. We argue that $x^2 \equiv a \pmod{p^n}$ is solvable by inducting on n. If $n = 1$, there is really nothing to prove; indeed, $(a/p) = 1$ is just another way of saying that $x^2 \equiv a \pmod{p}$ can be solved. Assume that the result holds for $n = k \geq 1$, so that $x^2 \equiv a \pmod{p^k}$ admits a solution x_0. Then

$$x_0^2 = a + bp^k$$

for an appropriate choice of b. In passing from k to $k + 1$, we shall use x_0 and b to write down explicitly a solution to the congruence $x^2 \equiv a \pmod{p^{k+1}}$.

Toward this end, we first solve the linear congruence

$$2x_0 y \equiv -b \pmod{p}$$

obtaining a unique solution y_0 modulo p (this is possible because $\gcd(2x_0, p) = 1$). Next, consider the integer

$$x_1 = x_0 + y_0 p^k.$$

Upon squaring this integer, we get

$$\begin{aligned}(x_0 + y_0 p^k)^2 &= x_0^2 + 2x_0 y_0 p^k + y_0^2 p^{2k} \\ &= a + (b + 2x_0 y_0) p^k + y_0^2 p^{2k}.\end{aligned}$$

But $p \mid (b + 2x_0 y_0)$, from which it follows that

$$x_1^2 = 1(x_0 + y_0 p^k)^2 \equiv a \pmod{p^{k+1}}.$$

Thus, the congruence $x^2 \equiv a \pmod{p^n}$ has a solution for $n = k + 1$ and, by induction, for all positive integers n. □

Example 1. Find a solution of the quadratic congruence

$$x^2 \equiv 23 \pmod{7^3}.$$

Theorem 9.4.2. *Let a be an odd integer. Then we have the following:*

(a) $x^2 \equiv a \pmod 2$ *always has a solution.*

(b) $x^2 \equiv a \pmod 4$ *has a solution if and only if* $a \equiv 1 \pmod 4$.

(c) $x^2 \equiv a \pmod{2^n}$, *for* $n \geq 3$, *has a solution if and only if* $a \equiv 1 \pmod 8$.

Proof. The first assertion is obvious. The second depends on the observation that the square of any odd integer is congruent to 1 modulo 4. Consequently, $x^2 \equiv a \pmod 4$ can be solved only when a is of the form $4k + 1$; in this event, there are two solutions modulo 4, namely, $x = 1$ and $x = 3$.

Now consider the case in which $n \geq 3$. Because the square of any odd integer is congruent to 1 modulo 8, we see that for the congruence $x^2 \equiv a \pmod{2^n}$ to be solvable a must be of the form $8k + 1$. To go the other way, let us suppose that $a \equiv 1 \pmod 8$ and proceed by induction on the exponent n. When $n = 3$, the congruence $x^2 \equiv a \pmod{2^n}$ is certainly solvable; indeed, each of the integers 1, 3, 5, 7 satisfies $x^2 \equiv 1 \pmod 8$. Fix a value of $n \geq 3$ and assume, for the induction hypothesis, that the congruence $x^2 \equiv a \pmod{2^n}$ admits a solution x_0. Then there exists an integer b for which

$$x_0^2 = a + b2^n.$$

Because a is odd, so is the integer x_0. It is therefore possible to find a unique solution y_0 of the linear congruence

$$x_0 y \equiv -b \pmod 2.$$

We argue that the integer

$$x_1 = x_0 + y_0 2^{n-1}$$

satisfies the congruence $x^2 \equiv a \pmod{2^{n+1}}$. Squaring yields

$$\begin{aligned}(x_0 + y_0 2^{n-1})^2 &= x_0^2 + x_0 y_0 2^n + y_0^2 2^{2n-2} \\ &= a + (b + x_0 y_0) 2^n + y_0^2 2^{2n-2}.\end{aligned}$$

By the way y_0 was chosen, $2 \mid (b + x_0 y_0)$; hence,

$$x_1^2 = (x_0 + y_0 2^{n-1})^2 \equiv a \pmod{2^{n+1}}$$

(we also use the fact that $2n - 2 = n + 1 + (n - 3) \geq n + 1$). Thus, the congruence $x^2 \equiv a \pmod{2^{n+1}}$ is solvable, completing the induction step and the proof. □

Theorem 9.4.3. *Let $n = 2^{k_0} p_1^{k_1} \cdots p_r^{k_r}$ be the prime factorization of $n > 1$ and let $\gcd(a, n) = 1$. Then $x^2 \equiv a \pmod n$ is solvable if and only if*

(a) $(a/p_i) = 1$ *for* $i = 1, 2, \ldots, r$;

(b) $a \equiv 1 \pmod 4$ *if* $4 \mid n$, *but* $8 \nmid n$; $a \equiv 1 \pmod 8$ *if* $8 \mid n$.

Example 2. Find the solutions of $x^2 + 5x + 6 \equiv 0 \pmod{5^3}$ and $x^2 + x + 3 \equiv 0 \pmod{3^3}$.

Example 3. Prove that if the congruence $x^2 \equiv a \pmod{2^n}$, where a is odd and $n \geq 3$, has a solution, then it has exactly four incongruent solutions.

Chapter 11

Numbers of Special Form

11.2 Perfect Numbers

Definition 11.2.1. A positive integer n is said to be perfect if n is equal to the sum of all its positive divisors, excluding n itself.

Example 1. Prove that the integer $n = 2^{10}(2^{11} - 1)$ is not a perfect number by showing that $\sigma(n) \neq 2n$.

Example 2. If n is a perfect number, prove that

$$\sum_{d|n} 1/d = 2.$$

Theorem 11.2.1. *If $2^k - 1$ is prime ($k > 1$), then $n = 2^{k-1}(2^k - 1)$ is perfect and every even perfect number is of this form.*

Proof. Let $2^k - 1 = p$, a prime, and consider the integer $n = 2^{k-1}p$. Inasmuch as $\gcd(2^{k-1}, p) = 1$, the multiplicativity of σ (as well as Theorem 6.1.2) entails that

$$\begin{aligned}\sigma(n) &= \sigma(2^{k-1}p) = \sigma(2^{k-1})\sigma(p)\\ &= (2^k - 1)(p + 1)\\ &= (2^k - 1)2^k = 2n,\end{aligned}$$

making n a perfect number.

For the converse, assume that n is an even perfect number. We may write n as $n = 2^{k-1}m$, where m is an odd integer and $k \geq 2$. It follows from $\gcd(2^{k-1}, m) = 1$ that

$$\sigma(n) = \sigma(2^{k-1}m) = \sigma(2^{k-1})\sigma(m) = (2^k - 1)\sigma(m),$$

whereas the requirement for a number to be perfect gives

$$\sigma(n) = 2n = 2^k m.$$

Together, these relations yield

$$2^k m = (2^k - 1)\sigma(m),$$

which is simply to say that $(2^k - 1) \mid 2^k m$. But $2^k - 1$ and 2^k are relatively prime, whence $(2^k - 1) \mid m$; say, $m = (2^k - 1)M$. Now the result of substituting this value of m into the last-displayed equation and canceling $2^k - 1$ is that $\sigma(m) = 2^k M$. Because m and M are both divisors of m (with $M < m$), we have

$$2^k M = \sigma(m) \geq m + M = 2^k M,$$

leading to $\sigma(m) = m + M$. The implication of this equality is that m has only two positive divisors, to wit, M and m itself. It must be that m is prime and $M = 1$; in other words, $m = (2^k - 1)M = 2^k - 1$ is a prime number. □

***Lemma* 11.2.1:** If $a^k - 1$ is prime ($a > 0$, $k \geq 2$), then $a = 2$ and k is also prime.

Proof. It can be verified without difficulty that

$$a^k - 1 = (a-1)(a^{k-1} + a^{k-2} + \cdots + a + 1)$$

where, in the present setting,

$$a^{k-1} + a^{k-2} + \cdots + a + 1 \geq a + 1 > 1.$$

Because by hypothesis $a^k - 1$ is prime, the other factor must be 1; that is, $a - 1 = 1$ so that $a = 2$.

If k were composite, then we could write $k = rs$, with $1 < r$ and $1 < s$. Thus,

$$\begin{aligned} a^k - 1 &= (a^r)^s - 1 \\ &= (a^r - 1)(a^{r(s-1)} + a^{r(s-2)} + \cdots + a^r + 1) \end{aligned}$$

and each factor on the right is plainly greater than 1. But this violates the primality of $a^k - 1$, so that by contradiction k must be prime. □

Theorem 11.2.2. *An even perfect number n ends in the digit 6 or 8; equivalently, either $n \equiv 6 \pmod{10}$ or $n \equiv 8 \pmod{10}$.*

Proof. Being an even perfect number, n may be represented as $n = 2^{k-1}(2^k - 1)$, where $2^k - 1$ is a prime. According to the last lemma, the exponent k must also be prime. If $k = 2$, then $n = 6$, and the asserted result holds. We may therefore confine our attention to the case $k > 2$. The proof falls into two parts, according as k takes the form $4m + 1$ or $4m + 3$.

If k is of the form $4m + 1$, then

$$\begin{aligned} n &= 2^{4m}(2^{4m+1} - 1) \\ &= 2^{8m+1} - 2^{4m} = 2 \cdot 16^{2m} - 16^m. \end{aligned}$$

A straightforward induction argument will make it clear that $16^t \equiv 6 \pmod{10}$ for any positive integer t. Utilizing this congruence, we get

$$n \equiv 2 \cdot 6 - 6 \equiv 6 \pmod{10}.$$

Now, in the case in which $k = 4m + 3$,

$$\begin{aligned} n &= 2^{4m+2}(2^{4m+3} - 1) \\ &= 2^{8m+5} - 2^{4m+2} = 2 \cdot 16^{2m+1} - 4 \cdot 16^m. \end{aligned}$$

Falling back on the fact that $16^t \equiv 6 \pmod{10}$, we see that

$$n \equiv 2 \cdot 6 - 4 \cdot 6 \equiv -12 \equiv 8 \pmod{10}.$$

Consequently, every even perfect number has a last digit equal to 6 or to 8. □

Example 3. If $\sigma(n) = kn$, where $k \geq 3$, then the positive integer n is called a k-perfect number (sometimes multiply perfect). Establish the following assertions concerning k-perfect numbers:

(a) $523776 = 2^9 \cdot 3 \cdot 11 \cdot 31$ is 3-perfect.
$30240 = 2^5 \cdot 3^3 \cdot 5 \cdot 7$ is 4-perfect.
$14182439040 = 2^7 \cdot 3^4 \cdot 5 \cdot 7 \cdot 11^2 \cdot 17 \cdot 19$ is 5-perfect.

(b) If n is a 3-perfect number and $3 \nmid n$, then $3n$ is 4-perfect.

(c) If n is a 5-perfect number and $5 \nmid n$, then $5n$ is 6-perfect.

(d) If $3n$ is a $4k$-perfect number and $3 \nmid n$, then n is $3k$-perfect.

For each k, it is conjectured that there are only finitely many k-perfect numbers. The largest one discovered has 558 digits and is 9-perfect.

11.3 Mersenne Primes and Amicable Numbers

Remark 1. Numbers of the form

$$M_n = 2^n - 1 \qquad n \geq 1$$

are called Mersenne numbers. Those Mersenne numbers that happen to be prime are said to be Mersenne primes.

Theorem 11.3.1. *If p and $q = 2p + 1$ are primes, then either $q \mid M_p$ or $q \mid M_p + 2$, but not both.*

Proof. With reference to Fermat's theorem, we know that

$$2^{q-1} - 1 \equiv 0 \pmod{q}$$

and, factoring the left-hand side, that

$$\begin{aligned}(2^{(q-1)/2} - 1)(2^{(q-1)/2} + 1) &= (2^p - 1)(2^p + 1) \\ &\equiv 0 \pmod{q}.\end{aligned}$$

What amounts to the same thing:

$$M_p(M_p + 2) \equiv 0 \pmod{q}.$$

The stated conclusion now follows directly from Theorem 3.1.1. We cannot have both $q \mid M_p$ and $q \mid M_p + 2$, for then $q \mid 2$, which is impossible. □

Theorem 11.3.2. *If $q = 2n + 1$ is prime, then we must have the following:*

(a) $q \mid M_n$, provided that $q \equiv 1 \pmod 8$ or $q \equiv 7 \pmod 8$.

(b) $q \mid M_n + 2$, provided that $q \equiv 3 \pmod 8$ or $q \equiv 5 \pmod 8$.

Proof. To say that $q \mid M_n$ is equivalent to asserting that

$$2^{(q-1)/2} = 2^n \equiv 1 \pmod{q}.$$

In terms of the Legendre symbol, the latter condition becomes the requirement that $(2/q) = 1$. But according to Theorem 9.2.5, $(2/q) = 1$ when we have $q \equiv 1 \pmod 8$ or $q \equiv 7 \pmod 8$. The proof of (b) proceeds along similar lines. □

Corollary 11.3.1. *If p and $q = 2p+1$ are both odd primes, with $p \equiv 3 \pmod 4$, then $q \mid M_p$.*

Proof. An odd prime p is either of the form $4k+1$ or $4k+3$. If $p = 4k+3$, then $q = 8k+7$ and Theorem 11.3.2 yields $q \mid M_p$. In the case in which $p = 4k+1$, $q = 8k+3$ so that $q \nmid M_p$. □

Theorem 11.3.3. *If p is an odd prime, then any prime divisor of M_p is of the form $2kp+1$.*

Proof. Let q be any prime divisor of M_p, so that $2^p \equiv 1 \pmod{q}$. If 2 has order k modulo q (that is, if k is the smallest positive integer that satisfies $2^k \equiv 1 \pmod{q}$), then Theorem 8.1.1 tells us that $k \mid p$. The case $k = 1$ cannot arise; for this would imply that $q \mid 1$, an impossible situation. Therefore, because both $k \mid p$ and $k > 1$, the primality of p forces $k = p$.

In compliance with Fermat's theorem, we have $2^{q-1} \equiv 1 \pmod{q}$, and therefore, thanks to Theorem 8.1.1 again, $k \mid q-1$. Knowing that $k = p$, the net result is $p \mid q-1$. To be definite, let us put $q - 1 = pt$; then $q = pt + 1$. The proof is completed by noting that if t were an odd integer, then q would be even and a contradiction occurs. Hence, we must have $q = 2kp+1$ for some choice of k, which gives q the required form. □

Theorem 11.3.4. *If p is an odd prime, then any prime divisor q of M_p is of the form $q \equiv \pm 1 \pmod{8}$.*

Proof. Suppose that q is a prime divisor of M_p, so that $2^p \equiv 1 \pmod{q}$. According to Theorem 11.3.3, q is of the form $q = 2kp + 1$ for some integer k. Thus, using Euler's criterion, $(2/q) \equiv 2^{(q-1)/2} \equiv 1 \pmod{q}$. whence $(2/q) = 1$. Theorem 9.2.5 can now be brought into play again to conclude that $q \equiv \pm 1 \pmod{8}$. □

Example 1. Prove that the Mersenne number M_{13} is a prime; hence, the integer $n = 2^{12}(2^{13} - 1)$ is perfect.

Example 2. Prove that the Mersenne number M_{29} is composite.

Theorem 11.3.5 (Euler)**.** *If n is an odd perfect number, then*

$$n = p_1^{k_1} p_2^{2j_2} \cdots p_r^{2j_r}$$

where the p_i's are distinct odd primes and $p_1 \equiv k_1 \equiv 1 \pmod 4$.

Proof. Let $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ be the prime factorization of n. Because n is perfect, we can write

$$2n = \sigma(n) = \sigma(p_1^{k_1})\sigma(p_2^{k_2}) \cdots \sigma(p_r^{k_r}).$$

Being an odd integer, either $n \equiv 1 \pmod 4$ or $n \equiv 3 \pmod 4$; in any event, $2n \equiv 2 \pmod 4$. Thus, $\sigma(n) = 2n$ is divisible by 2, but not by 4. The implication is that one of the $\sigma(p_i^{k_i})$, say $\sigma(p_1^{k_1})$, must be an even integer (but not divisible by 4), and all the remaining $\sigma(p_i^{k_i})$'s are odd integers.

For a given p_i, there are two cases to be considered: $p_i \equiv 1 \pmod 4$ and $p_i \equiv 3 \pmod 4$. If $p_i \equiv 3 \equiv -1 \pmod 4$, we would have

$$\begin{aligned}
\sigma(p_i^{k_i}) &= 1 + p_i + p_i^2 + \cdots + p_i^{k_i} \\
&\equiv 1 + (-1) + (-1)^2 + \cdots + (-1)^{k_i} \pmod 4 \\
&\equiv \begin{cases} 0 \pmod 4 & \text{if } k_i \text{ is odd} \\ 1 \pmod 4 & \text{if } k_i \text{ is even.} \end{cases}
\end{aligned}$$

Because $\sigma(p_1^{k_1}) \equiv 2 \pmod 4$, this tells us that $p_1 \not\equiv 3 \pmod 4$ or, to put it affirmatively, $p_1 \equiv 1 \pmod 4$. Furthermore, the congruence $\sigma(p_i^{k_i}) \equiv 0 \pmod 4$ signifies that 4 divides $\sigma(p_1^{k_1})$, which is not possible. The conclusion: if $p_i \equiv 3 \pmod 4$, where $i = 2, \ldots, r$, then its exponent k_i is an even integer.

Should it happen that $p_i \equiv 1 \pmod 4$—which is certainly true for $i = 1$—then

$$\begin{aligned}
\sigma(p_i^{k_i}) &= 1 + p_i + p_i^2 + \cdots + p_i^{k_i} \\
&\equiv 1 + 1^1 + 1^2 + \cdots + 1^{k_i} \pmod 4 \\
&\equiv k_i + 1 \pmod 4.
\end{aligned}$$

The condition $\sigma(p_1^{k_1}) \equiv 2 \pmod 4$ forces $k_1 \equiv 1 \pmod 4$. For the other values of i, we know that $\sigma(p_i^{k_i}) \equiv 1$ or $3 \pmod 4$, and therefore $k_i \equiv 0$ or $2 \pmod 4$; in any case, k_i is an even integer. The crucial point is that, regardless of whether $p_i \equiv 1 \pmod 4$ or $p_i \equiv 3 \pmod 4$, k_i is always even for $i \neq 1$. □

Corollary 11.3.2. *If n is an odd perfect number, then n is of the form*

$$n = p^k m^2$$

where p is a prime, $p \nmid m$, and $p \equiv k \equiv 1 \pmod 4$; in particular, $n \equiv 1 \pmod 4$.

Proof. The last assertion is the only non-obvious one. Because $p \equiv 1 \pmod 4$, we have $p^k \equiv 1 \pmod 4$. Notice that m must be odd; hence, $m \equiv 1$ or $3 \pmod 4$, and therefore upon squaring, $m^2 \equiv 1 \pmod 4$. It follows that

$$n = p^k m^2 \equiv 1 \cdot 1 \equiv 1 \pmod 4.$$ □

Example 3. If n is an odd perfect number, prove that n has at least three distinct prime factors.

11.4 Fermat Numbers

Definition 11.4.1. A Fermat number is an integer of the form

$$F_n = 2^{2^n} + 1 \qquad n \geq 0.$$

If F_n is prime, it is said to be a Fermat prime.

Theorem 11.4.1. *The Fermat number F_5 is divisible by* 641.

Proof. We begin by putting $a = 2^7$ and $b = 5$, so that

$$1 + ab = 1 + 2^7 \cdot 5 = 641.$$

It is easily seen that

$$1 + ab - b^4 = 1 + (a - b)^3 b = 1 + 3b = 2^4.$$

But this implies that

$$\begin{aligned} F_5 = 2^{2^5} + 1 &= 2^{32} + 1 \\ &= 2^4 a^4 + 1 \\ &= (1 + ab - b^4)a^4 + 1 \\ &= (1 + ab)a^4 + (1 - a^4 b^4) \\ &= (1 + ab)[a^4 + (1 - ab)(1 + a^2 b^2)], \end{aligned}$$

which gives $641 \mid F_n$. □

Theorem 11.4.2. *For Fermat numbers F_n and F_m, where $m > n \geq 0$,* $\gcd(F_m, F_n) = 1$.

Proof. Put $d = \gcd(F_m, F_n)$. Because Fermat numbers are odd integers, d must be odd. If we set $x = 2^{2^n}$ and $k = 2^{m-n}$, then

$$\begin{aligned} \frac{F_m - 2}{F_n} &= \frac{(2^{2^n})^{2^{m-n}} - 1}{2^{2^n} + 1} \\ &= \frac{x^k - 1}{x + 1} = x^{k-1} - x^{k-2} + \cdots - 1 \end{aligned}$$

whence $F_n \mid (F_m - 2)$. From $d \mid F_n$, it follows that $d \mid (F_m - 2)$. Now use the fact that $d \mid F_m$ to obtain $d \mid 2$. But d is an odd integer, and so $d = 1$. □

Theorem 11.4.3 (Pepin's test)**.** *For $n \geq 1$, the Fermat number $F_n = 2^{2^n} + 1$ is prime if and only if*

$$3^{(F_n - 1)/2} \equiv -1 \pmod{F_n}.$$

Proof. First let us assume that

$$3^{(F_n-1)/2} \equiv -1 \pmod{F_n}.$$

Upon squaring both sides, we get

$$3^{F_n-1} \equiv 1 \pmod{F_n}.$$

The same congruence holds for any prime p that divides F_n:

$$3^{F_n-1} \equiv 1 \pmod{p}.$$

Now let k be the order of 3 modulo p. Theorem 8.1.1 indicates that $k \mid F_n - 1$, or in other words, that $k \mid 2^{2^n}$; therefore k must be a power of 2.

It is not possible that $k = 2^r$ for any $r \leq 2^n - 1$. If this were so, repeated squaring of the congruence $3^k \equiv 1 \pmod{p}$ would yield

$$3^{2^{2^n-1}} \equiv 1 \pmod{p}$$

or, what is the same thing,

$$3^{(F_n-1)/2} \equiv 1 \pmod{p}.$$

We would then arrive at $1 \equiv -1 \pmod{p}$, resulting in $p = 2$, which is a contradiction. Thus the only possibility open to us is that

$$k = 2^{2^n} = F_n - 1.$$

Fermat's theorem tells us that $k \leq p - 1$, which means, in turn, that $F_n = k + 1 \leq p$. Because $p \mid F_n$, we also have $p \leq F_n$. Together these inequalities mean that $F_n = p$, so that F_n is a prime.

On the other hand, suppose that F_n, $n \geq 1$, is prime. The Quadratic Reciprocity Law gives

$$(3/F_n) = (F_n/3) = (2/3) = -1$$

when we use the fact that $F_n \equiv (-1)^{2^n} + 1 = 2 \pmod{3}$. Applying Euler's Criterion, we end up with

$$3^{(F_n-1)/2} \equiv -1 \pmod{F_n}.$$ □

Theorem 11.4.4. *Any prime divisor p of the Fermat number $F_n = 2^{2^n} + 1$, where $n \geq 2$, is of the form $p = k \cdot 2^{n+2} + 1$.*

Proof. For a prime divisor p of F_n,

$$2^{2^n} \equiv -1 \pmod{p}$$

which is to say, upon squaring, that

$$2^{2^{n+1}} \equiv 1 \pmod{p}.$$

If h is the order of 2 modulo p, this congruence tells us that

$$h \mid 2^{n+1}.$$

We cannot have $h = 2^r$ where $1 \leq r \leq n$, for this would lead to

$$2^{2^n} \equiv 1 \pmod{p}$$

and, in turn, to the contradiction that $p = 2$. This lets us conclude that $h = 2^{n+1}$. Because the order of 2 modulo p divides $\phi(p) = p - 1$, we may further conclude that $2^{n+1} \mid p-1$. The point is that for $n \geq 2$, $p \equiv 1 \pmod{8}$, and therefore, by Theorem 9.2.5, the Legendre symbol $(2/p) = 1$. Using Euler's criterion, we immediately pass to

$$2^{(p-1)/2} \equiv (2/p) = 1 \pmod{p}.$$

An appeal to Theorem 8.1.1 finishes the proof. It asserts that $h \mid (p-1)/2$, or equivalently, $2^{n+1} \mid (p-1)/2$. This forces $2^{n+2} \mid p - 1$, and we obtain $p = k \cdot 2^{n+2} + 1$ for some integer k. □

Example 1. Composite integers n for which $n \mid 2^n - 2$ are called pseudoprimes. Show that every Fermat number F_n is either prime or a pseudoprime.

Example 2. For $n \geq 2$, show that the last digit of the Fermat number $F_n = 2^{2^n} + 1$ is 7.

Example 3. Establish that $2^{2^n} - 1$ has at least n distinct prime divisors.

Index

Bibliography

[1] David M. Burton. *Elementary Number Theory Seventh Edition.* McGraw-Hill, 2011. Print.